4

“SITUACIÓN ACTUAL DE LA RED LAN DEL C.C.H. VALLEJO”

4.1 REQUERIMIENTOS Y NECESIDADES ACTUALES

4.1.1 APLICACIONES DE LOS USUARIOS

La red LAN del Plantel Vallejo del Colegio de Ciencias y Humanidades, tiene principalmente dos objetivos: el primero es proporcionar servicios tecnológicos y educativos a los alumnos del colegio para facilitar sus labores académicas. El segundo se refiere a las labores administrativas necesarias para el control de las actividades generales del plantel y su relación con otras instituciones.

Con la finalidad de cumplir éstas funciones, en cuestiones de administración, los usuarios que hacen uso de la red se encuentran distribuidos en 27 departamentos correspondientes a 10 áreas directivas, las cuales se alojan en 13 edificios. Dentro de estas instalaciones se tienen 100 usuarios fijos y otros tantos que hacen uso de salas de cómputo las cuales cuentan con 71 estaciones de trabajo. Se tienen además 3 servidores locales, para contar con un total de 174 nodos de usuario que conforman la red.

Mediante la red se proporcionan servicios básicos de conexión entre computadoras, las cuales de manera individual no requieren alta demanda de ancho de banda, como lo pudiera representar, mencionándolo a manera de ejemplo, un servicio de videoconferencia de alta calidad.

Área	Departamento	Usuarios
Dirección	Dirección	5
	Secretaría particular	
	Secretarias	
Unidad de planeación	Jefatura del área	3
Unidad jurídica	Jefatura del área	1
Secretaría general	Jefatura del área	2
	Información	
Secretaría académica	Jefatura del área	88
	Audiovisual	
	Biblioteca	
	Sistemas	
	Salas de cómputo	
Secretaría docente	Jefatura del área	15
	Sección de experimentales	
	Sección Histórico-social	
	Sección de talleres	
Secretaría técnica del Siladin	Jefatura del área	27
	CENAD	
	Creatividad	
Secretaría de Asuntos estudiantiles	Jefatura del área	7
	Psico-pedagogía	
Secretaría de administración escolar	Control escolar	12
Secretaría administrativa	Jefatura del área	14
	Personal docente	
	Personal administrativo	
	Control presupuestal	
	Aprovisionamiento e inventarios	
	Librería	
	Residencia de obras	

Tabla 4.1: Áreas administrativas en las que se dividen los usuarios de la red LAN del C.C.H. Vallejo.

En cuanto a la utilización, aunque en mayor o menor grado, básicamente el uso que todas las áreas hacen de la red es del mismo tipo, el cual está basado en la consulta de correo electrónico y de información mediante páginas Web, acceso a bases de datos almacenadas en un servidor local, transferencia de mensajes de texto, así como el compartimento de recursos (impresoras o espacio en disco) que se traduce en la transferencia de archivos de manera local.

De estos servicios, de acuerdo a entrevista con los propios usuarios, los más usados son la consulta HTTP, correo electrónico y la transferencia de archivos entre nodos locales. En lo que se refiere a la consulta y envío de correo electrónico, este servicio a su vez hace uso del protocolo HTTP mediante páginas en sitios Web, ya que la mayoría de las cuentas de los usuarios corresponden a servicios proporcionados por empresas que ofrecen esta modalidad.

Se determinó además que el mayor uso de la red corresponde a la Secretaría Administrativa, en específico los departamentos de Control Presupuestal y Aprovisionamiento e Inventarios, así como la Secretaría Académica, a través de los salones de cómputo, en los cuales los alumnos realizan sus investigaciones accediendo a Internet durante todo el periodo de actividades del plantel. Esto no indica que el resto de los departamentos no empleen los servicios de red a diario, sino que la utilización corresponde a periodos más reducidos durante el día.

4.2 ESTRUCTURA DE LA RED.

4.2.1 TIPO DE RED.

Para la interconexión de su equipo de computo, la red LAN empleada en el plantel Vallejo es del tipo Ethernet, lo que implica una velocidad de transferencia entre dispositivos de 10 Mbps.

Como equipos de conexión se utilizan tanto concentradores como switches, por lo cual existe alguna división de los dominios de colisión en ciertos segmentos de la red, pero no de la manera más adecuada, sobre todo por la ubicación de los concentradores principales en la topología.

Respecto al tipo de cableado, el uso de fibra óptica es requerido para la unión de ciertos equipos de conexión, así como el par trenzado de cobre UTP, éste último sobre todo para la conexión de nodos finales. Todo lo anterior será analizado más a fondo en secciones posteriores.

Por otra parte, en lo que se refiere al servicio de conexión hacia una red WAN, es decir, el tipo de conexión a Internet, es proporcionado por un servicio conocido como DS0, cuya máxima velocidad de transferencia es de 64 kbps. Debido a que no existe restricción alguna en ningún nodo para el acceso a Internet, este es el ancho de banda disponible para todos los usuarios conectados a la red.

4.2.2 EQUIPO DE CONEXIÓN (HARDWARE).

Dentro de esta red existe un equilibrio aproximado de la cantidad de concentradores y switches empleados, contándose con un total de 15 de los primeros por un total de 11 de los segundos.

4.2.2.1 CONCENTRADORES.

Por parte de estos dispositivos, se cuenta con tres diferentes marcas, las cuales son 3COM, Intellinet y Cabletron Systems. La tabla 4.2 muestra la cantidad de concentradores existentes por cada una de estas marcas.

CONCENTRADORES		
Marca	**Modelo**	**Cantidad**
3COM	OfficeConnect Dual Speed	1
	LinkBuilder FMS II	3
	Super Stack	1
	Super Stack II PS Hub 40	3
Intellinet	5 Port 10Base-T	1
	5 Port Dual Speed	2
Cabletron Systems	MRXI	3
	MiniMMAC	1

Tabla 4.2: Cantidad por marcas de concentradores.

A continuación se mencionan las principales características de los diferentes modelos de las distintas marcas de concentradores con los que se cuenta:

- **3COM**

  - OfficeConnect Dual Speed:

    Puertos: 16 para conectores R-J45
    Protocolo de enlace de datos: Ethernet, Fast Ethernet
    Velocidad de transmisión: 10/100 Mbps
    Estándares aceptados: IEEE 802.3, IEEE 802.3u
    Otras características: Modo de comunicación Half-duplex y Full-duplex

  - LinkBuilder FMS II:

    Puertos: 24 para conectores RJ-45, 1 AUI integrado y 1 interfaz transreceptora de fibra óptica.
    Protocolo de enlace de datos: Ethernet
    Velocidad de transmisión: 10 Mbps
    Estándares aceptados: IEEE 802.3, ISO 8802/3

  - Super Stack
    Puertos; 12 para conectores RJ-45, 1 interfaz transreceptora de fibra óptica.
    Protocolo de enlace de datos: Ethernet.
    Velocidad de transmisión: 10 Mbps.
    Estándares aceptados: IEEE 802.3

- Super Stack II PS HUB 40

  Puertos: 24 para conectores RJ-45, 2 interfaces transreceptoras de fibra óptica.
  Protocolo de enlace de datos: Ethernet
  Velocidad de transmisión: 10 Mbps.
  Estándares aceptados: IEEE 802.3

- **Intellinet**

  - Ethernet 10BaseT

    Puertos: 5+1 para conectores RJ-45 (1 para enlace con otros equipos)
    Protocolo de enlace de datos: Ethernet
    Velocidad de transmisión: 10 Mbps.
    Estándares aceptados: IEEE 802.3
    Otras características: Apilable hasta 4 unidades.

  - 5 Port Dual Speed

- **Cabletron Systems**

  - MRXI

    Puertos: 12 para conectores RJ-45
    Protocolo de enlace de datos: Ethernet
    Velocidad de transmisión: 10 Mbps
    Estándares aceptados: IEEE 802.3
    Otras características: Soporte para administración mediante SNMP

  - MiniMMAC

    Puertos: 12 de Fibra óptica, 1 interfaz coaxial
    Protocolo de enlace de datos: Ethernet
    Velocidad de transmisión: 10 Mbps
    Estándares aceptados: IEEE 802.3

4.2.2.2 SWITCHES.

Los modelos de switches usados en la red actual proporcionan, en su mayoría, funciones básicas correspondientes a este tipo de dispositivos, esto es, que no cuentan con soporte de estándares más específicos del tratamiento de la información, como lo puede ser la segmentación en VLAN's o bien la prioridad de entrega de paquetes.

Para el caso de estos dispositivos también se cuenta con tres marcas: 3COM, C-NET y Genius. La descripción correspondiente a estos equipos es la siguiente:

SWITCHES		
Marca	**Modelo**	**Cantidad**
3COM	OfficeConnect Dual Speed	7
	Baseline 10/100	1
C-NET		2
Genius	Fast Ethernet N-Way	1

Tabla 4.3: Cantidad por marcas y modelos de switches.

- **3COM**

  - Office Conect Dual Speed

    Puertos: 16 para conectores RJ-45
    Protocolo de enlace de datos: Ethernet, Fast Ethernet
    Velocidad de transmisión: 10/100 Mbps
    Estándares aceptados: IEEE 802.3, IEEE 802.3u
    Otras características: 1 MB de RAM, modos de transmisión Half-duplex y Full-duplex

  - Baseline 10/100

    Puertos: 8 RJ-45
    Protocolo de enlace de datos: Ethernet, Fast Ethernet
    Velocidad de transmisión: 10/100 Mbps
    Estándares aceptados: IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1p
    Otras características: Modo de transmisión Full-duplex

- **C-NET**

  - CNSH-800

    Puertos: 8 para conectores RJ-45
    Protocolo de enlace de datos: Ethernet, Fast Ethernet
    Velocidad de transmisión: 10/100Mbps
    Estándares aceptados: IEE802.3, IEEE802.3u
    Otras características: Latencia de 2.7 ms a 100Mbps y 13 ms a 10 Mbps, memoria de 1M, transmisión en modos Full-duplex y Half-duplex.

- **Genius:**

  - Fast Ethernet N Way GS4080 Mini

    Puertos: 8 para conectores RJ-45.
    Protocolo de enlace de datos: Ethernet, Fast Ethernet.
    Velocidad de transmisión: 10/100 Mbps.
    Estándares aceptados: IEEE 802.3, IEEE 802.3u.

Otras características: Transmisión Half-duplex y Fullduplex, método de reenvío de tramas "store and forward", tabla de direcciones para 1000 registros.

4.2.2.3 ENRUTADORES.

En esta red se cuenta únicamente con un enrutador, el cual se trata de un equipo marca Cisco, modelo 2501 quien es el que recibe el servicio de DS0 proporcionado por un módem marca Adtron, modelo ISU 2x64. Las principales características de este modelo de enrutador son las siguientes:

- **Especificaciones técnicas**

  - Puertos: 1 Ethernet para conector RJ-45, 2 seriales, 1 AUI.
  - Procesador: Motorola 68030 a 20 MHz.
  - Memoria: Flash de 4 MB, DRAM de 4 MB.
  - Software: IP/Bridging, IP/IPX/AT.
  - Enrutamiento: RIP, IP, IGRP, OSPF, IPX, IPX Spoofing, AppleTalk 1y 2, AURP
  - Administración de red: Cisco Vision 1.0 (requiere una PC con S.O. Windows 3.1 o superior).
  - Administaración inteligente mediante SNMP y Telnet. Un puerto de consola para configuración y uno auxiliar para administración fuera de banda.

- **Cisco IOS**

El Cisco IOS (Internetwork Operating System) es un sistema operativo de interconexión de redes que, de acuerdo a las especificaciones del fabricante, permite lo siguiente:

  - Enrutamiento TCP/IP, Novell IPX y AppleTalk
  - Enlace de tipo puente transparente
  - Seguridad de acceso a la red
  - Compresión de datos
  - Optimización del ancho de banda de la red de área amplia (WAN)

- **Aplicaciones**

  Las ventajas proporcionadas por cada una de las siguientes características se mencionan de acuerdo a lo descrito por la empresa Cisco:

  - Enrutamiento Dial-on-Demand
  - El enrutamiento sobre demanda (DDR) proporciona conexión WAN solo cuando es necesario. DDR beneficia a los sitios remotos que requieren acceso ocasional a los servicios de la red. Esto reduce el costo del acceso de área amplia usando ISDN o líneas seriales de marcado ("dial-up") como alternativas a las líneas contratadas. Esta característica trabaja con ambientes IP, IPX y Apple Talk.
  - Optimización del ancho de banda
  - Soporta diversas características de optimización, con una compresión de datos arriba de una relación 4:1 para velocidades de transmisión WAN superiores a 128 kbps.

4.2.3 TOPOLOGÍA ACTUAL Y TIPO DE CABLEADO.

Al tratarse de una red Ethernet, estamos hablando de una topología lógica de bus; sin embargo, como se ha mencionado en ocasiones anteriores, esto no necesariamente corresponde a la misma topología física. Para este caso, más adelante será posible observar que se trata de una topología física del tipo jerárquica o de árbol, de acuerdo a la conexión que existe entre los concentradores y switches existentes, y de éstos a su vez con los respectivos nodos de usuario.

El servicio de salida a Internet se proporciona por un módem DS0 el cual es conectado mediante cable serial a un enrutador, que a su vez se enlaza a través de cable coaxial a un concentrador principal, mismo que funciona a manera de red dorsal colapsada, encargada de hacer la distribución de cableado hacia el resto de los edificios donde se ubican los diferentes equipos a los cuales se encuentran conectados los usuarios.

Debido a las distancias entre edificios conectados a la red, que son superiores a los 100 metros en la mayoría de los casos, el cableado empleado para llevar el servicio desde el concentrador principal hacia los demás edificios se trata de fibra óptica. En este punto, dentro de los edificios, a través de los equipos de conexión correspondientes ya es posible realizar una distribución haciendo uso de par trenzado de cobre UTP para conectar tanto nodos de usuario como otros concentradores y/o switches en cascada, quienes son los encargados de proporcionar servicio a otros usuarios finales.

En la figura 4.1 se puede observar un plano general del plantel Vallejo del C.C.H, el cual permite ubicar los distintos edificios que cuentan con servicio de red de los que conforman el complejo escolar, así como las trayectorias que debe seguir el cableado entre estos edificios, de acuerdo a la posición de los registros construidos para tal propósito.

Según se aprecia en el plano, la ubicación del equipo principal se encuentra dentro del edificio "J", lo que indica que a partir de dicho edificio se hace la distribución del servicio de red al resto del plantel. Es por ello que desde este punto se deben considerar las distancias que recorre el cableado por cada segmento para llegar a otro edificio, y por tanto verificar el límite de distancia de 100 metros en la que se puede hacer uso de cable UTP. Se analizará entonces, de acuerdo a las distancias, la razón por la cual se usa cada tipo de cableado en la actualidad. La tabla 4.4 contiene las longitudes existentes entre edificios y el tipo de cable que se usa para conectarlos:

Trayectoria	***Longitud [m]***	***Tipo de cable usado***
Edificio J – Audiovisual (CREPA)	324	Fibra óptica
Edificio J – Sria. Servicios Estudiantiles (S.S.E)	336	Fibra óptica
Edificio J – Biblioteca	501	Fibra óptica
Edificio J – Edificio Y	303	Fibra óptica
Edificio J – Siladin A	505	Fibra óptica
Edificio J – Siladin B	505	Fibra óptica
Edificio J – Dirección	94	Fibra óptica
Dirección – Edificio M	74	UTP
Audiovisual (CREPA) – Edificio J	75	UTP
Edificio J – Edificio G	36	UTP
Edificio G – Edificio E	10	UTP
Edificio Y – Edificio Z	71	UTP
Siladin A – Almacén	91	UTP

Tabla 4.4: Distancias entre edificios y cable utilizado.

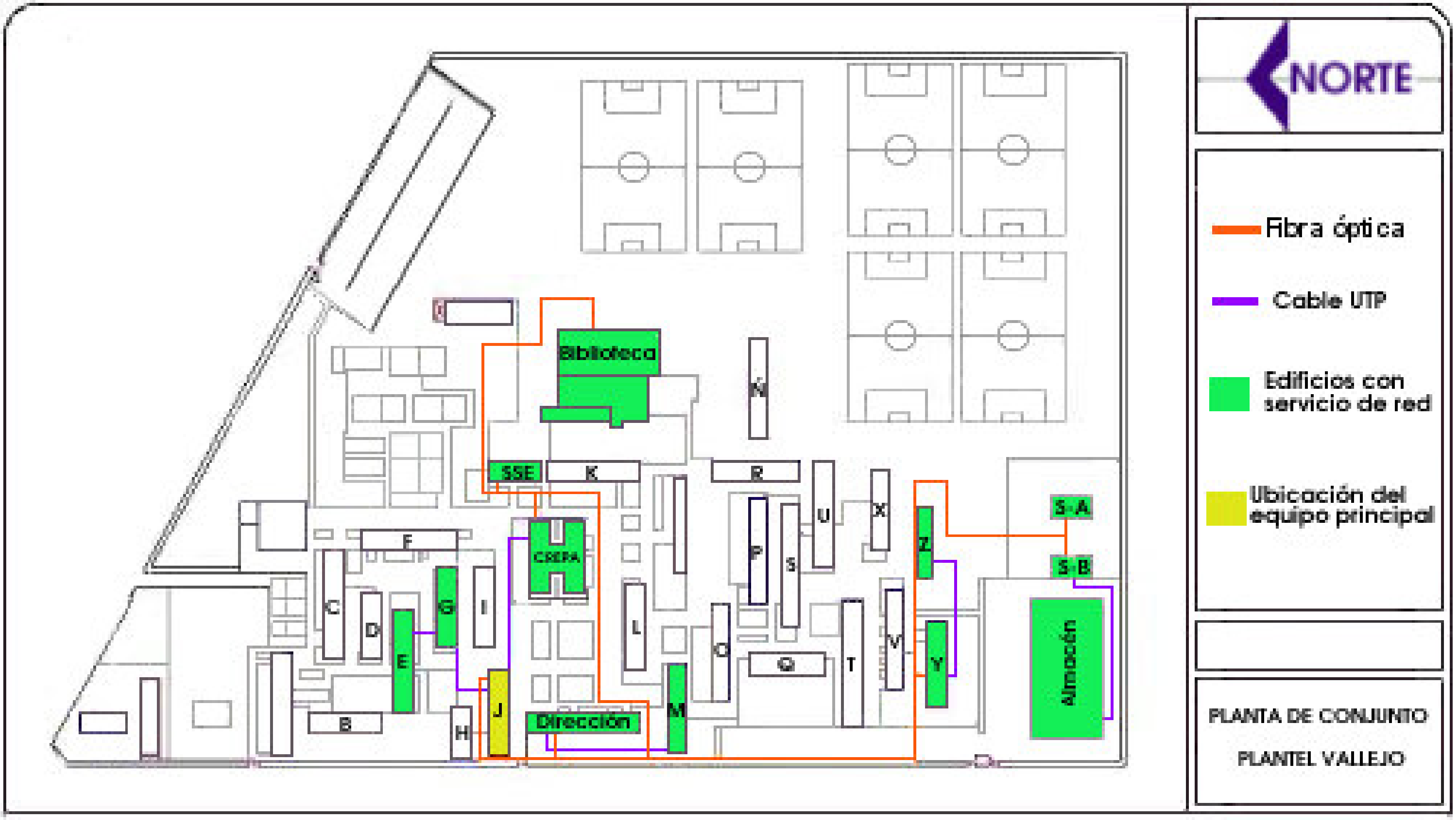

Figura 4.1: Plano general del plantel Vallejo con trayectorias de cableado entre edificios.

Se observa la presencia de 8 trayectorias que parten del edificio “J”, siete de las cuales están cubiertas por fibra óptica. Estas trayectorias son las consideradas como los enlaces principales, por llamarlos de algún modo. En uno de estos enlaces, el que va del edificio “J” al edificio de la Dirección, a pesar de que tiene una longitud menor a los 100 metros, se hace uso también de fibra óptica; la razón, muy probablemente de acuerdo a las condiciones originales de diseño, se debe al concentrador que se utiliza para proporcionar estos enlaces, el cual cuenta únicamente con puertos de fibra óptica (Cabletron Systems MiniMMAC).

En el resto de los enlaces se emplea par trenzado de cobre UTP, haciendo una conexión de equipos en cascada para proporcionar servicio de red a otros edificios a partir de los que previamente se conectaban mediante fibra óptica (de los edificios “Y”, Audiovisual, Siladin “A” y Dirección, a los edificios “Z”, “J”, Almacén y “M” respectivamente). En los casos de los edificios “G” y “E”, la conexión se hace a partir de un enlace de cascada doble, es decir, una conexión en cascada a partir del equipo de un edificio que en un punto anterior es conectado de esta misma forma a otro en un edificio distinto. En otras palabras, para estos edificios involucrados, la conexión es de la siguiente forma: del Audiovisual al edificio “J” y de este último al edificio “G”, que a su vez se conecta finalmente al edificio “E”

Es necesario señalar que si se analiza la tabla 4.4, se nota la existencia dos distintos enlaces entre el edificio “J” y el Audiovisual. En primera instancia se debe aclarar que se tienen longitudes diferentes para estos enlaces debido a las trayectorias que siguen las respectivas conexiones, según se observa en el plano de la figura 4.1.

La razón de la presencia de estas dos trayectorias es que la primera se debe a la conexión mediante fibra óptica que establece el enlace entre el concentrador principal ubicado en el edificio “J” y el respectivo del Audiovisual. La segunda trayectoria existe debido al enlace establecido desde el concentrador del Audiovisual hacia un segundo concentrador de puertos RJ-45 para cable UTP también ubicado en el edificio “J”, responsable de proporcionar servicio a otro concentrador de este mismo edificio para conectar a los usuarios respectivos del área.

Además del edificio “J”, es en los “Y”, Siladin B, Dirección, Biblioteca y Secretaria de Servicios Estudiantiles donde se realiza una conexión a partir del concentrador principal del edificio para enlazar otros dispositivos, ya sea concentradores y/o switches con el propósito de cubrir todos los usuarios dentro de cada edificio.

Con el fin de tener más clara esta información, así como para complementar la misma con los dispositivos no mencionados anteriormente con exactitud de cantidad ubicados dentro de cada edificio, es necesario construir un esquema en el que se visualice la totalidad de las conexiones, además de la ubicación de todos y cada uno de los equipos de conexión existentes. Para ello, la 4.2 proporciona el diagrama de la red.

Un punto que no debe pasarse por alto es la ubicación de los servidores dentro de la topología, ya que se trata de elementos que generan mayor tránsito de información que las estaciones de trabajo y por tanto debe tomarse en cuenta su posición en la red, y sobre todo conocer si se encuentran conectados a concentradores o switches. De acuerdo al esquema que se presentará, los tres servidores de la red se encuentran conectados a los equipos D1, SB2 y S2, respectivamente. Solamente el que se encuentra conectado a D1 es accedido por diversos nodos de la red, mientras que los otros dos se tratan de servidores locales al segmento en el que se ubican.

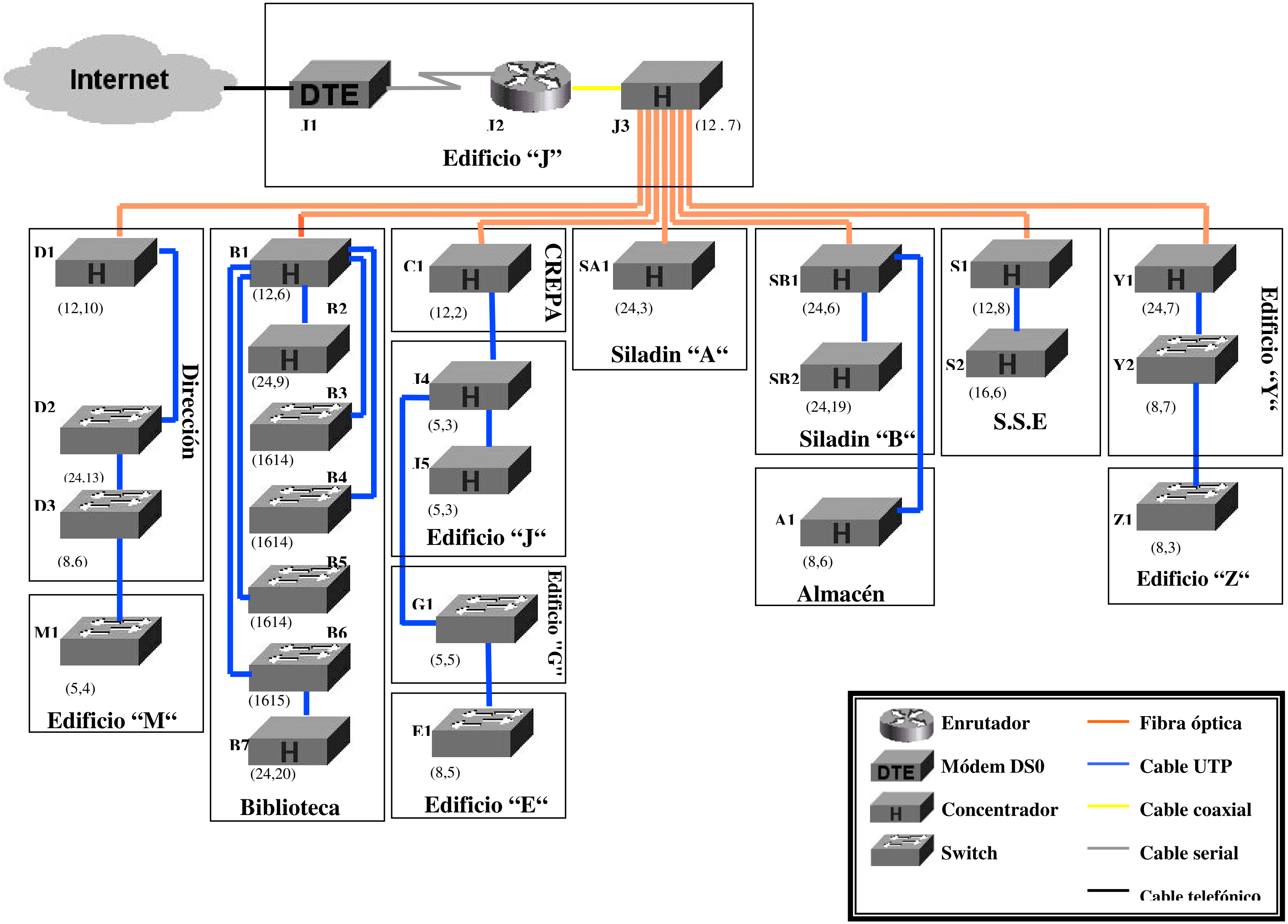

Figura 4.2: Topología de la red LAN del C.C.H. Vallejo

En este diagrama se tiene una pareja de números entre paréntesis acompañando a cada equipo de conexión. La primer cantidad en cada caso indica el número total de puertos del dispositivo, mientras que la segunda da a conocer la cantidad de dichos puertos que son utilizados para establecer tanto los enlaces hacia nodos de usuario, como los requeridos desde y hacia otros equipos de conexión.

Una vez presentado el diagrama, lo único que resta para tener conocimiento total de la estructura es hacer la indicación correspondiente del equipo especifico que se ubica en cada edificio. Con este objeto, a continuación se listan los edificios con los respectivos dispositivos, nombrados de acuerdo a las etiquetas asociadas a cada elemento en la figura 4.2:

- **Edificio "J" (equipo principal)**
  J1: Módem DS0 Adtran ISU 2x64
  J2: Enrutador Cisco Pro Access Solutions 2501
  J3: Concentrador Cabletron Systems MiniMMAC

- **Dirección.**
  D1: Concentrador Cabletron Systems MRXI
  D2: Switch C-NET CNSH-800
  D3: Switch 3COM Baseline 10/100

- **Edificio "M"**
  M1: Switch 3COM OfficeConnect Dual Speed

- **Biblioteca**
  B1: Concentrador Cabletron Systems MRXI
  B2: Concentrador Link Builder FMS II
  B3-B6: 4 Switches 3COM OfficeConnect Dual Speed
  B7: Concentrador Link Builder FMS II

- **Audiovisual (CREPA)**
  C1: Concentrador 3COM Super Stack

- **Edificio J (equipo de usuarios)**
  J4, J5: 2 concentradores Intellinet 5 Port Dual Speed

- **Edificio "G"**
  G1: Switch 3COM OfficeConnect

- **Edificio "E"**
  E1: Switch Genius Fast Ethernet N-Way

- **Siladin "A"**
  SA1: Concentrador 3COM Super Stack II PS Hub 40

- **Siladin "B"**
  SB1, SB2: 2 concentradores 3COM Super Stack II PS Hub 40

- **Almacén**
  A1: Concentrador 5 Port 10Base-T

- **Secretaría de Asuntos Estudiantiles**
  S1: Concentrador Cabletron Systems MRXI
  S2: Concentrador OfficeConnect Dual Speed

- **Edificio "Y"**
  Y1: Concentrador 3COM Link Builder FMS II
  Y2: Switch 3COM OfficeConnect

- **Edificio "Z"**
  Z1: Switch C-NET CNSH-800

4.3 MONITORIZACIÓN DE LA RED.

Hasta el momento se ha dado a conocer la estructura de la red, así como el equipo de conexión que la conforma y el tipo de cableado usado. Sin embargo, falta aún conocer el aspecto lógico, lo cual se logra analizando el flujo de información considerando su tipo, de acuerdo a la información generada por los diversos protocolos que sean utilizados y la metodología de comunicación que requieran, puedan o deban usar éstos, ya sea difusión general, multidifusión o transmisión dedicada a un nodo.

También es necesario conocer los posibles problemas en alguno o varios de los segmentos de la red ocasionados por todo este flujo de datos. Como ejemplo de ello se puede hacer presente una gran cantidad de colisiones, retransmisión excesiva de datos, así como “cuellos de botella”; todos ellos factores muy relacionados en muchos de los casos. Esta información será de gran utilidad para diagnosticar los principales dificultades que no permitan un desempeño óptimo de la red, lo cual servirá para facilitar la propuesta de un diseño de reestructuración que logre solucionar de la manera más eficiente todas las situaciones indeseables.

4.3.1 SOFTWARE EMPLEADO PARA LA MONITORIZACIÓN.

La metodología para conocer los datos referentes al flujo de información es conectarse como un nodo en diversos segmentos de la red analizada, haciendo uso de software especializado para tales propósitos.

Este tipo de programas conocidos como “sniffers”, a través de la tarjeta de red de la computadora, capturan la información que fluye y la traducen en estadísticas para su interpretación, ya sea de manera gráfica y/o a través de tablas.

El tipo y cantidad de información que proporcionan estos programas varía entre cada uno de ellos. Es por esta situación que para el análisis de la red LAN del C.C.H. Vallejo se emplearon cinco diferentes programas con la finalidad de complementar y corroborar la información obtenida.

De los programas puestos a prueba para el análisis, el software empleado se seleccionó por la facilidad de interpretación de diversos datos obtenidos. Los nombres de los cinco programas elegidos son Netasyst, Commview, Agilent Advisor, Distinct Network Monitor y Ultra Network Sniffer. Las características e información proporcionada por cada uno de estos programas es mas extensa que la enunciada a continuación, sin embargo los datos mencionados fueron los utilizados:

- **Netasyst**

  Se trata de un software muy completo, ya que además de los datos de monitorización, es capaz de analizar el contenido de las tramas capturadas. Se puede configurar el periodo de captura para las gráficas que genera.

  Datos que proporciona:
  - Total de paquetes y bytes circulados en la red.
  - Promedio de bytes por segundo
  - Cantidad de paquetes de broadcast y multicast de MAC, IP e IPX
  - Nivel de utilización de la red.
  - Reporte de errores y problemas de la red como tormentas de broadcast/multicast, exceso de retransmisiones y sesiones de protocolos rechazadas o sin respuesta.
  - Gráficas de comunicaciones entre nodos, así como colisiones, broadcast, multicast, paquetes y errores por segundo y porcentaje de protocolos utilizados.

- **CommView**

  Permite capturar gran cantidad de datos sobre la red analizada, la cual complementa con gráficas. Tiene como

opción la posibilidad de realizar la monitorización vía remota, aunque ciertas capturas de datos no se encuentran disponibles bajo esta modalidad.

Datos que proporciona:

- Promedio de paquetes y bytes por segundo.
- Total de paquetes y bytes circulados.
- Nivel de utilización de la red.
- Paquetes, bytes y promedio de bytes por segundo de entrada, salida y paso por la red.
- Total de paquetes y porcentaje correspondiente a cada protocolo.
- Distribución del tamaño de paquetes.
- Paquetes y bytes totales de broadcast y multicast, así como lo generado de este tipo en particular por cada nodo.
- Paquetes y bytes enviados y recibidos por cada nodo en su modo de dirección MAC y dirección IP.
- Cantidad de paquetes con errores.
- Cantidad de colisiones detectadas.
- Gráficas de la utilización del ancho de banda de la red, protocolos usados y distribución del tamaño de los paquetes.

- **Agilent Advisor**

Software similar a Netasyst, la diferencia radica en la presentación de los datos.

Datos que proporciona:

- Protocolos usados por cada nodo identificado por su dirección MAC y nombre en la red.
- Porcentaje del total de paquetes correspondientes a cada protocolo (IP, Novell, MAC)
- Paquetes detectados con colisiones.
- Cantidad y descripción de errores detectados.
- Gráficas del nivel de utilización de la red, colisiones, comunicación entre nodos

- **Distinct Network Monitor**:

Este programa es útil tanto para detectar problemas de funcionamiento en cada nodo en particular, como para la administración de la red en general, gracias a la monitorización que realiza de las actividades de los usuarios, pues permite observar el acceso a páginas Web mediante HTTP de cada nodo en particular.

Datos que proporciona:

- Total de paquetes y bytes capturados.
- Paquetes de entrada, salida y paso en la red.
- Paquetes y bytes enviados y recibidos, así como el total de los mismos por protocolo utilizado.
- Lista de nodos con sus respectivas comunicaciones y errores.
- Gráficas de la utilización del ancho de banda y protocolos usados

- **Ultra Network Sniffer**

  Está basado en gráficas, ya que todos los datos capturados los presenta de esta forma. También es capaz de decodificar las tramas capturadas.

  Datos que proporciona:

  - Gráfica del porcentaje de protocolos utilizados, incluyendo Ethernet, IP, TCP, UDP, ICMP, IGMP, ARP, IPX, HTTP, FTP, SMTP, DNS y otros.
  - Gráfica de la distribución de tamaño de paquetes.
  - Gráficas de porcentaje del total de paquetes enviados por cada nodo identificados por su dirección IP y MAC.

4.3.2 RESULTADOS DE LA MONITORIZACIÓN DE LA RED.

Para la lectura de datos se establecieron conexiones en distintos puntos de la red, con el fin de obtener resultados variados sobre el comportamiento del flujo de datos. Los puntos de conexión fueron determinados por dos situaciones: la primera fue la intención de cubrir la mayor extensión posible de la red, mientras que la segunda estuvo determinada por la accesibilidad del equipo de conexión. De esta forma, los dispositivos a los cuales se conectó el equipo de monitorización fueron B2, J4, SB2, A1 y S2; esta nomenclatura, por supuesto, de acuerdo al esquema de la topología de la figura 4.2.

4.3.2.1 PROTOCOLOS UTILIZADOS.

Los resultados de la lectura de los protocolos que operan en la red, son para la mayoría de los casos los esperados, ya que se emplean varios de los protocolos de la pila TCP/IP para efectuar la comunicación entre equipos, según se hace constar por las estadísticas determinadas por los programas utilizados.

Con el fin de contar con una referencia aún más aceptable de la actividad de los usuarios de la red, las lecturas de los datos se realizaron a lo largo del día considerando las horas más significativas del mismo; de acuerdo a esto, los datos presentados son los que resumen y muestran un mejor panorama de la actividad de la red.

- **Datos registrados en el Edificio J, equipo "J4".**

El programa "CommView" presenta los resultados de los protocolos analizados en tablas que contienen la cantidad de paquetes o bytes registrados durante el tiempo de captura de información. Los resultados son separados en dos tablas: una de los que el programa denomina "Protocolos IP" y otra con los "Sub-protocolos IP", siendo los primeros los correspondientes a la capa de transporte de la pila TCP/IP (TCP y UDP), así como ICMP e IGMP pertenecientes a la capa de red . Los que denomina "Subprotocolos IP" no son más que los protocolos correspondientes a la capa de aplicación.

En la información que a continuación se presenta, el texto que precede a los conjuntos de tablas corresponde al registro de control del programa analizador "CommView".

Reporte de Estadísticas *Generado sobre 26/04/2004 a 09:31:28 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:08*

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	90	2.4
UDP	3643	97.17
ICMP	12	0.32
IGMP	4	0.11

Tabla 4.5

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	750	0.14
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	439850	82.46
HTTPS	0	0
DNS	74693	14
Otros	18112	3.4

Tabla 4.6

Reporte de Estadísticas Generado sobre 26/04/2004 a 12:31:28 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:08

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	90	2.4
UDP	3643	97.17
ICMP	12	0.32
IGMP	4	0.11

Tabla 4.7

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	750	0.14
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	439850	82.46
HTTPS	0	0
DNS	74693	14
Otros	18112	3.4

Tabla 4.8

Reporte de Estadísticas Generado sobre 26/04/2004 a 02:58:23 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 02:00:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	2067	15.2
UDP	11473	84.34
ICMP	53	0.39
IGMP	10	0.07

Tabla 4.9

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	39169	1.93
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	1628875	80.2
HTTPS	0	0
DNS	207652	10.22
Otros	155413	7.65

Tabla 4.10

Reporte de Estadísticas Generado sobre 26/04/2004 a 04:20:28 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:08

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	3731	16.31
UDP	19041	83.21
ICMP	85	0.37
IGMP	25	0.11

Tabla 4.11

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	44819	1.32
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	2735349	80.7
HTTPS	0	0
DNS	253886	7.49
Otros	355286	10.48

Tabla 4.12

Reporte de Estadísticas Generado sobre 26/04/2004 a 07:20:15 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:08

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	5589	14.95
UDP	31627	84.57
ICMP	117	0.31
IGMP	63	0.17

Tabla 4.13

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	54791	1.05
FTP	0	0
POP3	0	
SMTP	0	0
Telnet	0	0
NetBIOS	4252515	81.44
HTTPS	0	0
DNS	346464	6.63
Otros	568136	10.88

Tabla 4.14

Tablas 4.5 – 4.14: Datos sobre los protocolos de la pila TCP/IP registrados en el equipo "J4"

Con la finalidad de apreciar mejor la presencia de los diferentes protocolos, las gráficas que enseguida se presentan permiten visualizar un comportamiento representativo de las muestras de datos presentadas en las tablas anteriores.

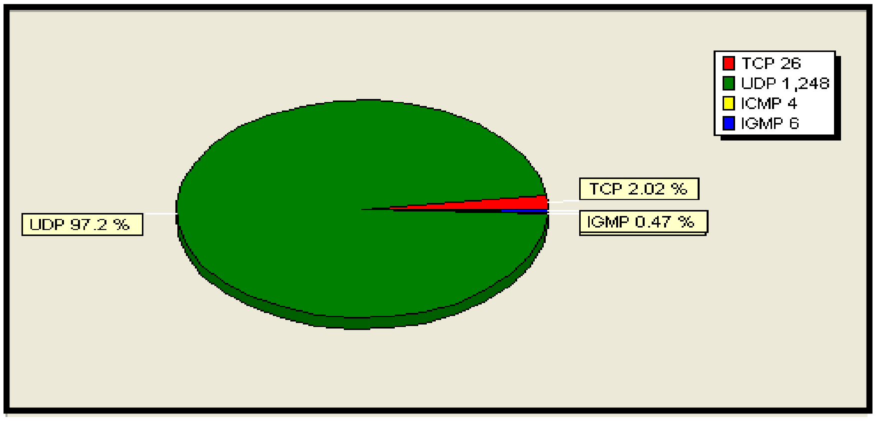

Figura 4.3: Gráfica de datos representativos correspondientes a los "Protocolos IP" de "CommView"

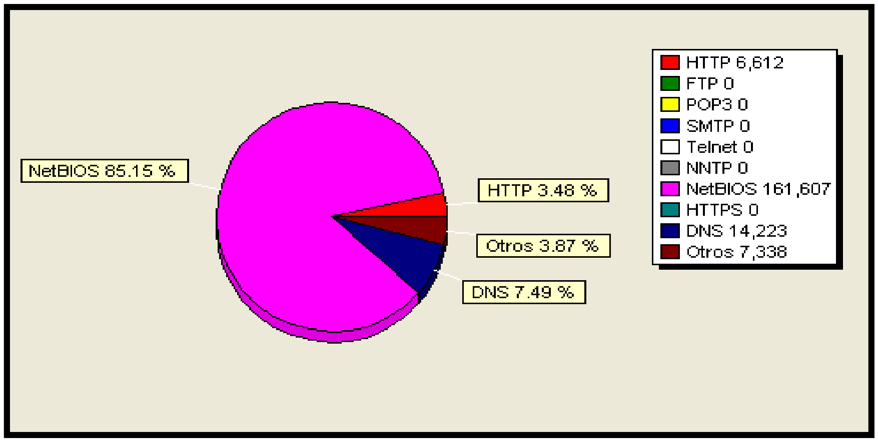

Figura 4.4: Gráfica de los "Subprotocolos IP" según datos de "Commview".

- **Datos registrados en la Biblioteca, equipo "B2"**

Reporte de Estadísticas Generado sobre 30/04/2004 a 08:00:00 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	40443	81.18
UDP	1302	2.61
ICMP	285	0.57
HBH-HEAD	7780	15.62
IGMP	6	0.01

Tabla 4.15

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	1601021	7.33
FTP	0	0.00
POP3	0	0.00
SMTP	0	0.00
Telnet	0	0.00
NetBIOS	75429	0.35
HTTPS	102638	0.47
DNS	92718	0.42
Otros	19974088	91.43

Tabla 4.16

Reporte de Estadísticas Generado sobre 28/04/2004 a 02:11:08 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	87716	69.63
UDP	26578	21.1
ICMP	3584	2.85
HBH-HEAD	8089	6.42
IGMP	8	0.01

Tabla 4.17

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	7866453	22.16
FTP	41942	0.12
POP3	112240	0.32
SMTP	0	0
Telnet	0	0
NetBIOS	817629	2.3
HTTPS	68645	0.19
DNS	2606713	7.34
Otros	23979442	67.56

Tabla 4.18

Reporte de Estadísticas Generado sobre 28/04/2004 a 04:06:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	102731	69.54
UDP	32321	21.88
ICMP	4728	3.2
HBH-HEAD	7935	5.37
IGMP	9	0.01

Tabla 4.19

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	12472322	33.96
FTP	30695	0.08
POP3	7058	0.02
SMTP	0	0
Telnet	0	0
NetBIOS	1371434	3.73
HTTPS	110019	0.3
DNS	3678393	10.02
Otros	19057452	51.89

Tabla 4.20

Reporte de Estadísticas Generado sobre 28/04/2004 a 07:06:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	11858	97.29
UDP	326	2.67
ICMP	0	0
HBH-HEAD	0	0
IGMP	4	0.03

Tabla 4.21

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	0	0
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	48172	1.8
HTTPS	0	0
DNS	0	0
Otros	2626083	98.2

Tabla 4.22

Reporte de Estadísticas Generado sobre 28/04/2004 a 08:36:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00.

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	311	93.67
UDP	21	6.33
ICMP	0	0

Tabla 4.23

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	0	0
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	2770	5.8
HTTPS	0	0
DNS	0	0
Otros	45012	94.2

Tabla 4.24

Tablas 4.15 – 4.24: Datos sobre los protocolos de la pila TCP/IP registrados en el equipo "B2"

La representación gráfica de la tendencia en la distribución de cantidad de información registrada en este caso corresponde a lo mostrado en las figuras presentadas a continuación:

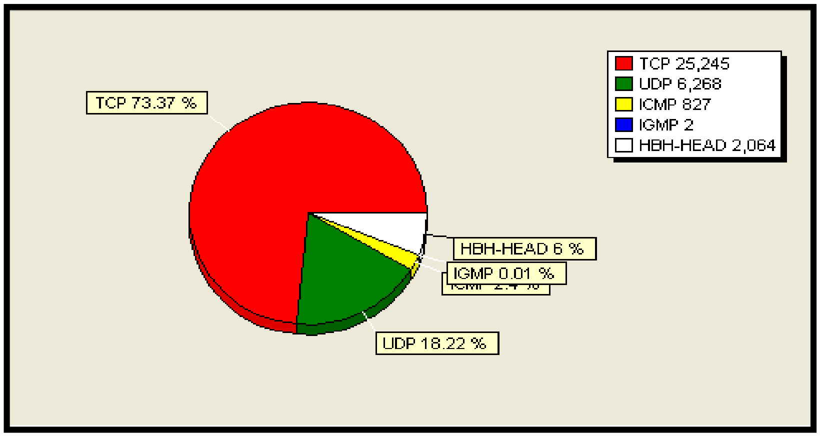

Figura 4.5: Gráfica de los "Protocolos IP" de Commview para el equipo "B ".

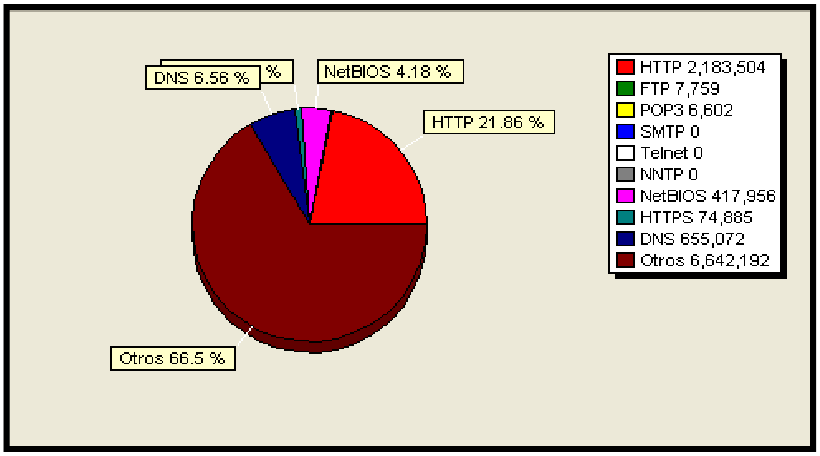

Figura 4.6: Gráfica de los "Sub-protocolos IP" de Commview para el equipo "B2".

Se aprecia en las tablas que el programa "Commview" solamente brinda información acerca de los protocolos de la pila TCP/IP, lo cual no significa que en la red no se empleen protocolos distintos a éstos. Para verificar la existencia de paquetes de otro tipo de protocolos se hizo uso del programa "Netasyst", el cual separa la lectura de información en tres categorías: MAC, IP e IPX. En la primer categoría se muestran los protocolos superiores al nivel MAC que son encapsulados en tramas de capa 2 del modelo OSI. Las categorías IP e IPX muestran los protocolos correspondientes a los conjuntos que operan bajo TCP/IP e IPX respectivamente.

Tomando una muestra de datos con este programa en el equipo correspondiente a ésta zona de la red ("B2"), la información obtenida es la siguiente:

MAC

Protocol	Packets	Bytes
IP	119613	30960894
IPX	4469	972770
IP_ARP	459	29376
NetBEUI	2023	416179
Others	3408	4883631

Tabla 4.25

IPX

Protocol	Packets	Bytes
NBIOS	2382	319446
NMPI1360	1515	561327
NMPI1361	200	23812
NRIP	80	5140
Others	239	56791
SAP	53	6254

Tabla 4.26

IP

Protocol	Packets	Bytes
Bootpc	12	3528
DNS	21337	3423610
FTP_Ctrl	458	50799
H225	2	160
HTTP	25651	9319675
HTTPS	325	95566
ICMP	4797	472201
NFS	5	450
NetBIOS_DGM_U	698	170949
NetBIOS_NS_U	1895	213942
NetBIOS_SSN_T	3212	421360
Others	61132	16776376
POP3	62	10066
XWin6000	27	2212

Tabla 4.27

Tablas 4.25 – 4.27: Registro de datos con el programa Netasyst para el equipo "B 2"

Estos mismos datos se pueden visualizar mediante las gráficas que enseguida se muestran:

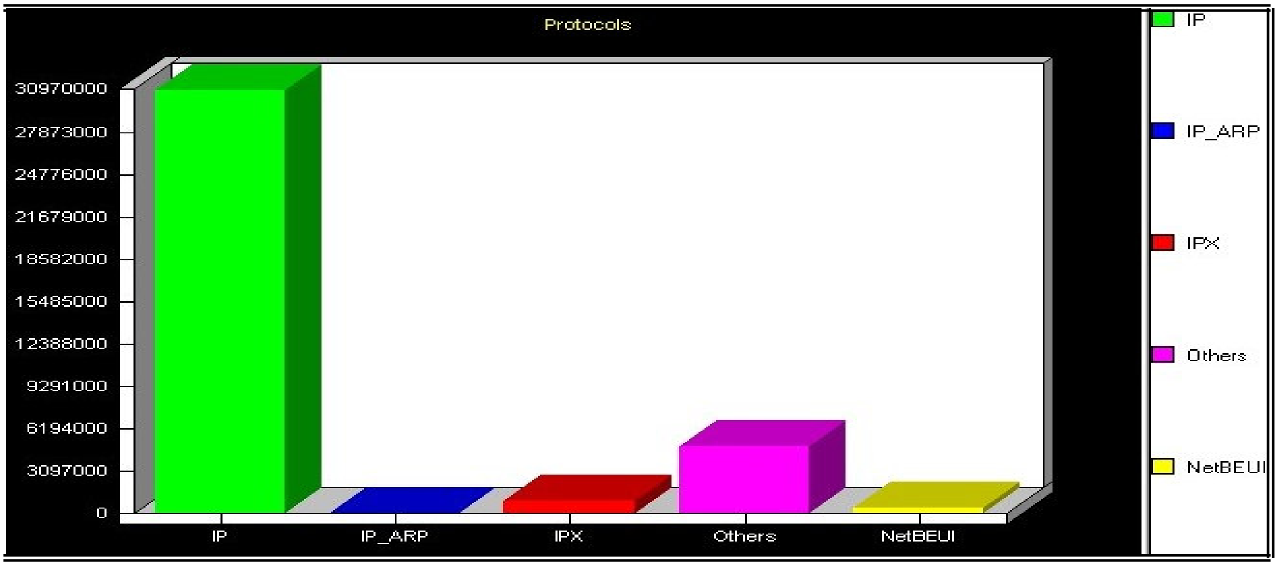

Figura 4.7: Protocolos superiores encapsulados en el nivel MAC presentados por "Netasyst".

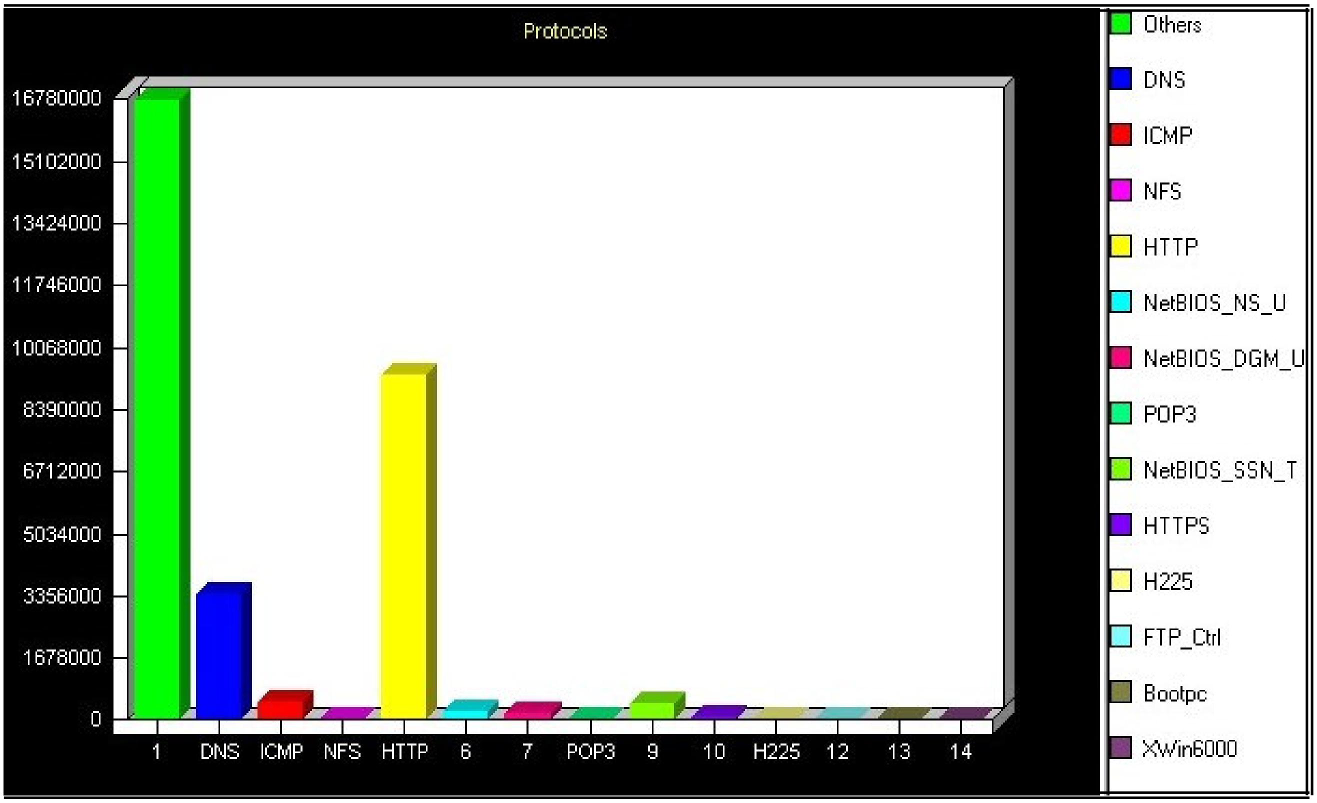

Figura 4.8: Protocolos de la categoría IP presentados por "Netasyst".

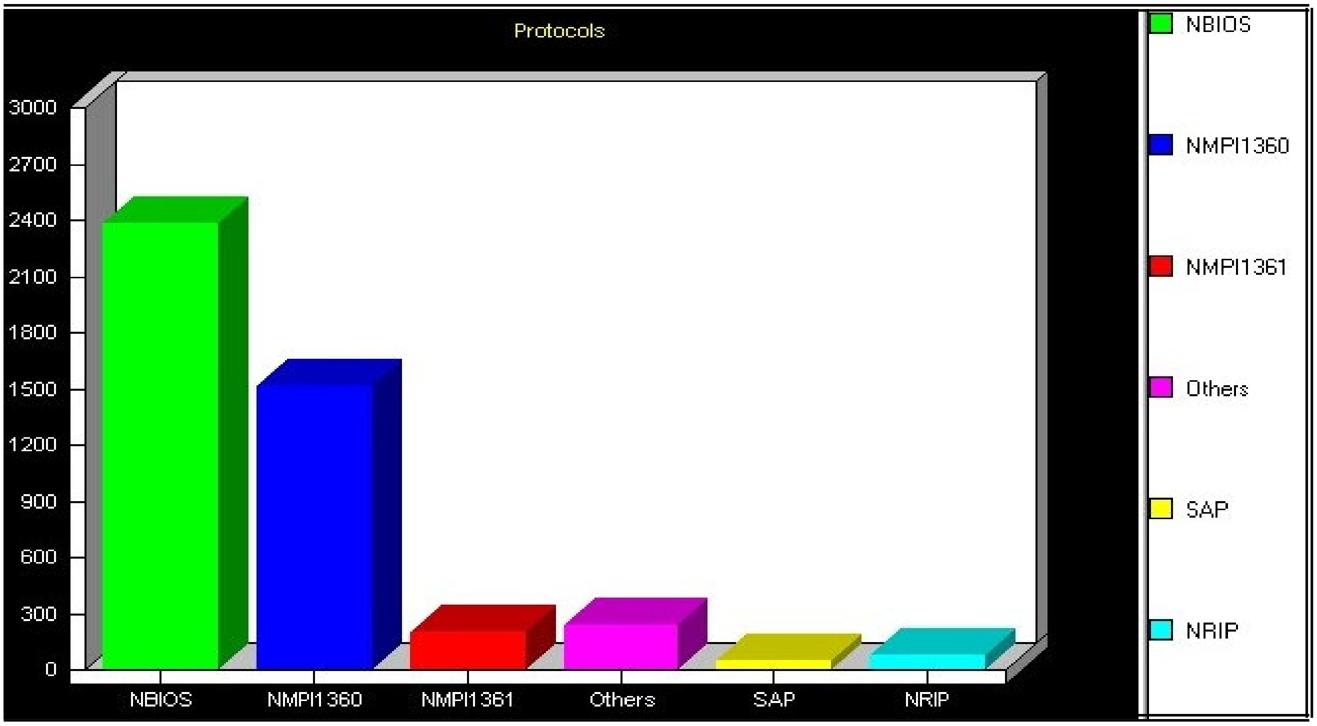

Figura 4.9: Protocolos de la categoría IPX presentados por "Netasyst".

Dado que "Netasyst" no muestra datos gráficos sobre los protocolos TCP y UDP, para estas categorías se hará uso en los casos posteriores de la información entregada por "CommView". En otra situación, analizando las gráficas de los protocolos de aplicación TCP/IP de "CommView" y "Netasyst", se aprecia que las gráficas no presentan grandes diferencias, por lo que en lo consiguiente se empleará solamente la información gráfica de "Netasyst" para presentar dicha información.

Por su parte, se tiene que el programa "Ultra Network Sniffer" engloba todos los protocolos detectados en una sola gráfica, incluyendo los de nivel MAC, que en este caso se trata de Ethernet, lo cual se visualiza en la figura 4.10. Lo significativo de esta gráfica es que permite observar cuales de los protocolos predominan de manera general en la red sin importar su categoría.

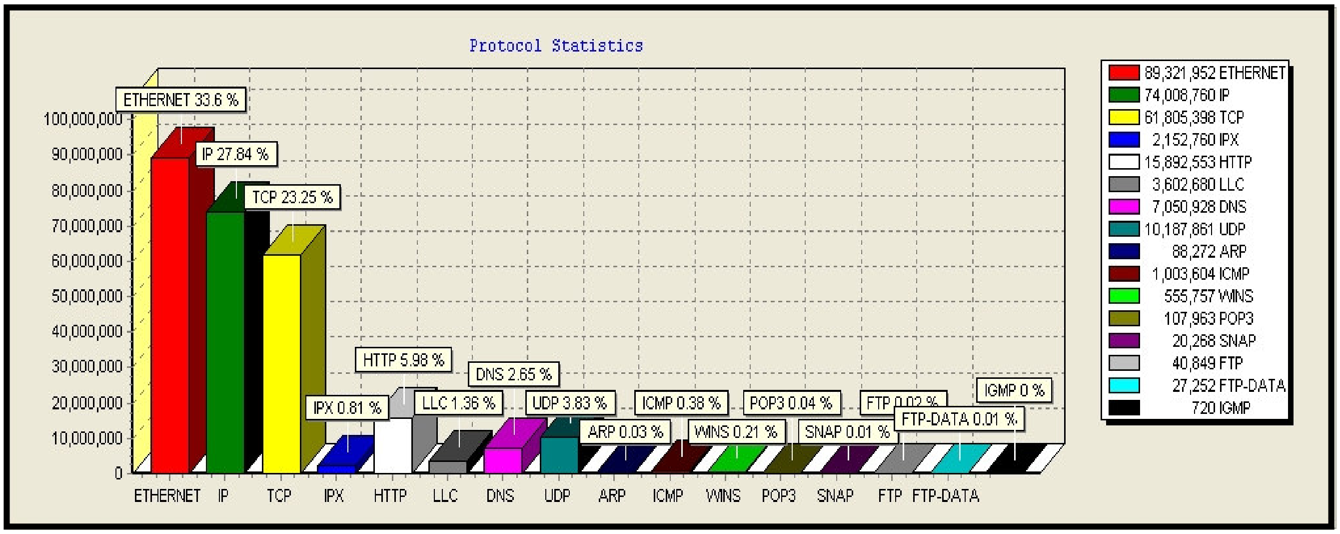

Figura 4.10: Gráfica general de protocolos generada por "Ultra Netwok Sniffer" para el equipo "B 2".

• Datos registrados en Siladin "B", equipo "SB2"

Reporte de Estadísticas Generado sobre 29/04/2004 a 10:00:00 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	49967	89.54
UDP	478	0.86
ICMP	174	0.31
HBH-HEAD	5181	9.28
IGMP	1	0

Tabla 4.28

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	2312695	9.05
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	20345	0.08
HTTPS	80185	0.31
DNS	59595	0.23
Otros	2307506290.32	

Tabla 4.29

Reporte de Estadísticas Generado sobre 29/04/2004 a 07:30:00 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	39899	80.3
UDP	1365	2.75
ICMP	302	0.61
HBH-HEAD	8121	16.34
IGMP	3	0.01

Tabla 4.30

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	1573201	7.11
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	65713	0.3
HTTPS	62462	0.28
DNS	122681	0.55
Otros	20307804	91.76

Tabla 4.31

Reporte de Estadísticas Generado sobre 29/04/2004 a 03:00:00 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	71516	74.57
UDP	15140	15.79
ICMP	1734	1.81
HBH-HEAD	7508	7.83
IGMP	5	0.01

Tabla 4.34

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	13344888	47.81
FTP	8914	0.03
POP3	2477	0.01
SMTP	1863	0.01
Telnet	0	0
NetBIOS	1469832	5.27
HTTPS	617214	2.21
DNS	1057672	3.79
Otros	11406615	40.87

Tabla 4.35

Reporte de Estadísticas Generado sobre 30/04/2004 a 11:30:00 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	62394	72.04
UDP	14415	16.64
ICMP	1864	2.15
IGMP	32	0.04
HBH-HEAD	7911	9.13

Tabla 4.32

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	6336830	23.42
FTP	6458	0.02
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	1185264	4.38
HTTPS	513418	1.9
DNS	909112	3.36
Otros	18105258	66.92

Tabla 4.33

Reporte de Estadísticas Generado sobre 29/04/2004 a 07:30:00 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	57008	79.51
UDP	7012	9.78
ICMP	2856	3.98
IGMP	1	0
HBH-HEAD	4822	6.73

Tabla 4.36

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	15863492	64.43
FTP	0	0
POP3	0	0
SMTP	0	0
Telnet	0	0
NetBIOS	390136	1.58
HTTPS	124413	0.51
DNS	170183	0.69
Otros	8074710	32.79

Tabla 4.37

Tablas 4.28 – 4.37: Datos sobre los protocolos de la pila TCP/IP registrados en el equipo "SB2"

Gráficamente tenemos el siguiente comportamiento con los protocolos TCP, UDP, ICMP, IGMP y HBH-HEAD:

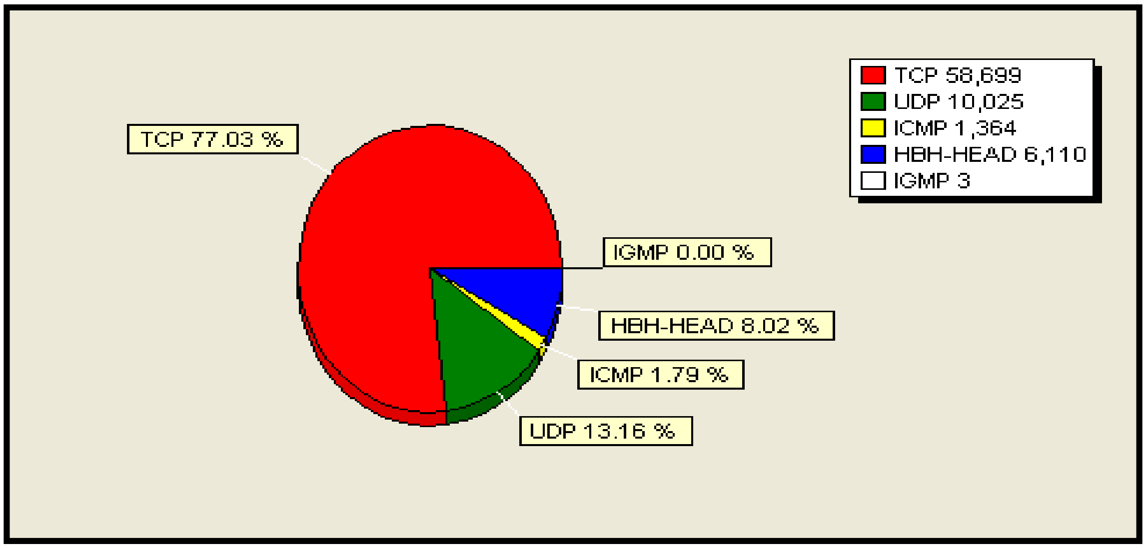

Figura 4.11: Protocolos registrados por “CommView” en el equipo “SB2“

De los protocolos superiores encapsulados en el nivel MAC registrados en este punto se presenta el siguiente comportamiento en esta zona de la red:

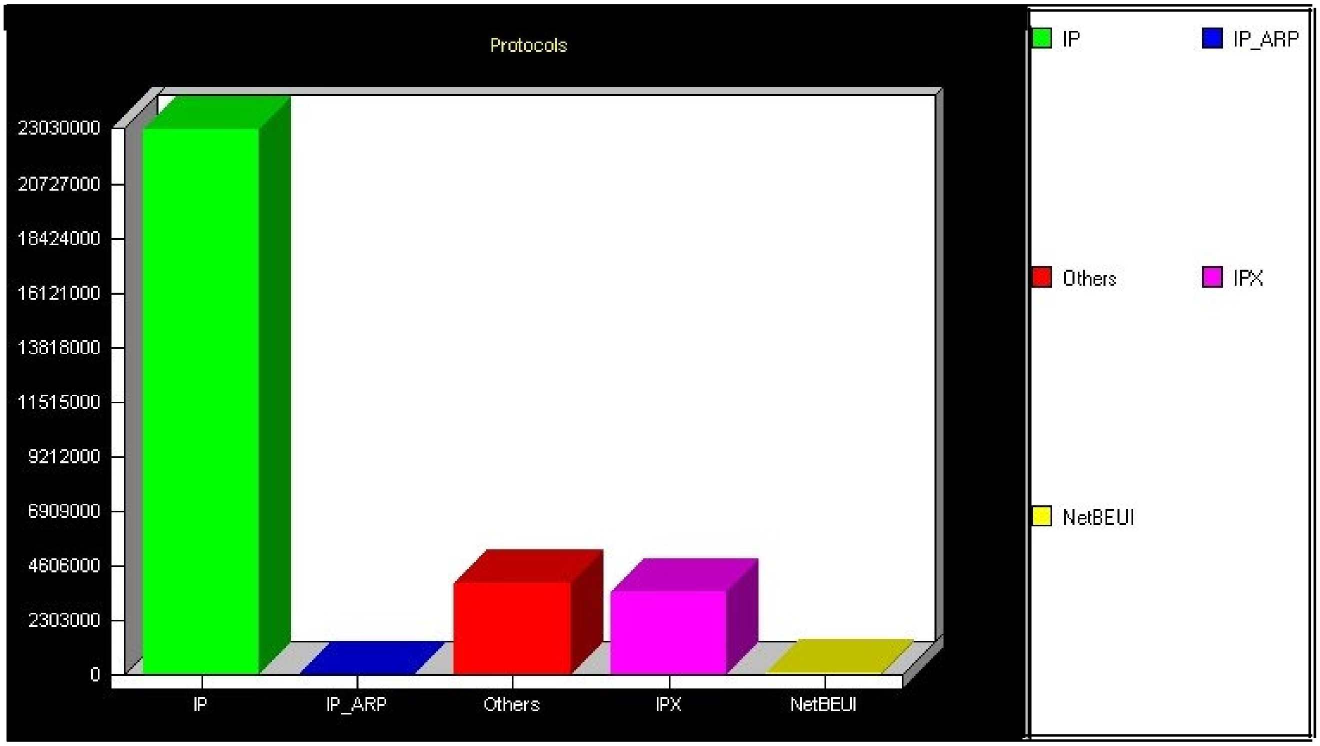

Figura 4.12: Protocolos encapsulados superiores al nivel MAC registrados en el equipo “SB2“.

Para el resto de los protocolos TCP/IP registrados en el equipo "SB2", de acuerdo a los datos representativos se tiene la distribución mostrada en la figura:

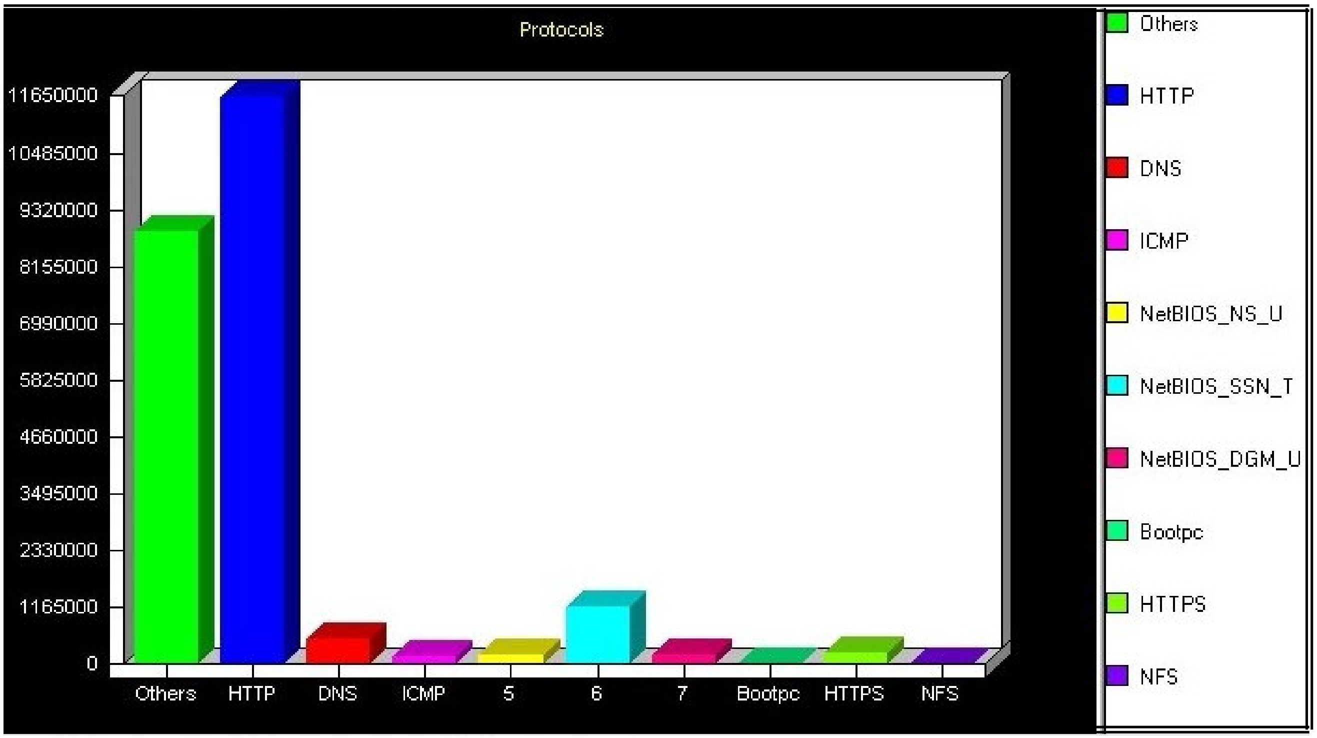

Figura 4.13: Protocolos de la pila TCP/IP registrados en el equipo "SB2 "

La distribución de los protocolos IPX registrados en este equipo se muestra en la gráfica siguiente:

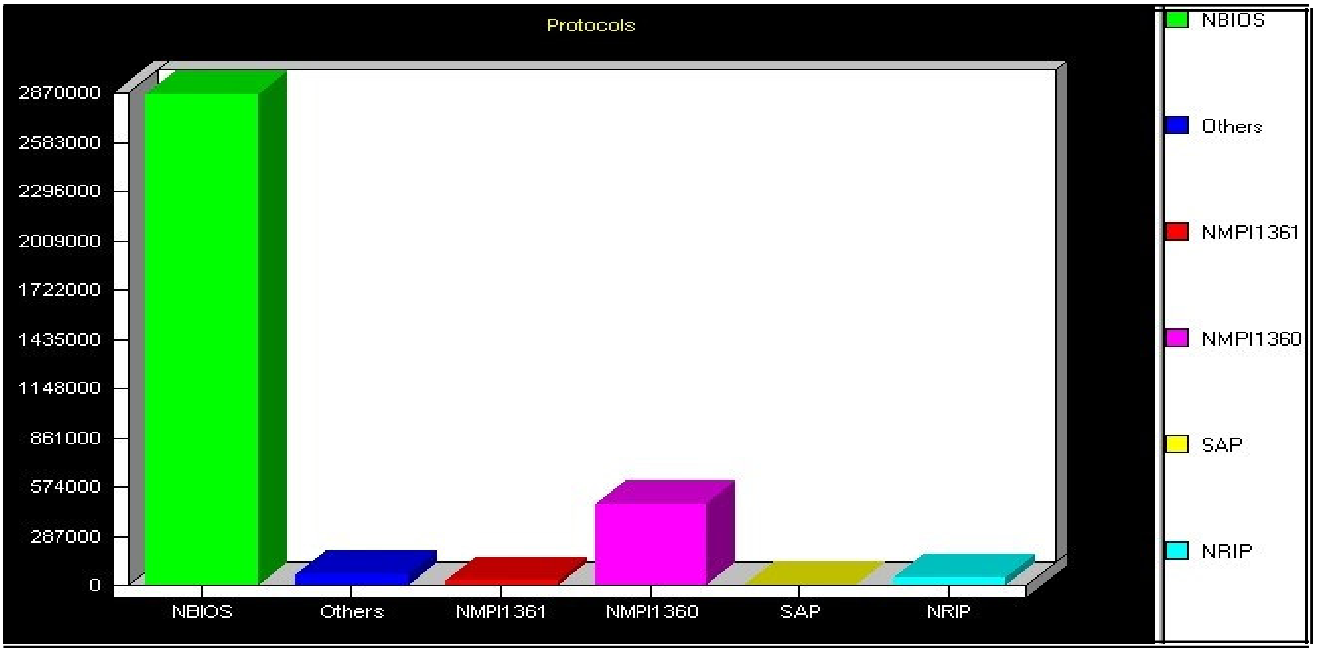

Figura 4.14: Protocolos del conjunto IPX registrados en el equipo "SB2"

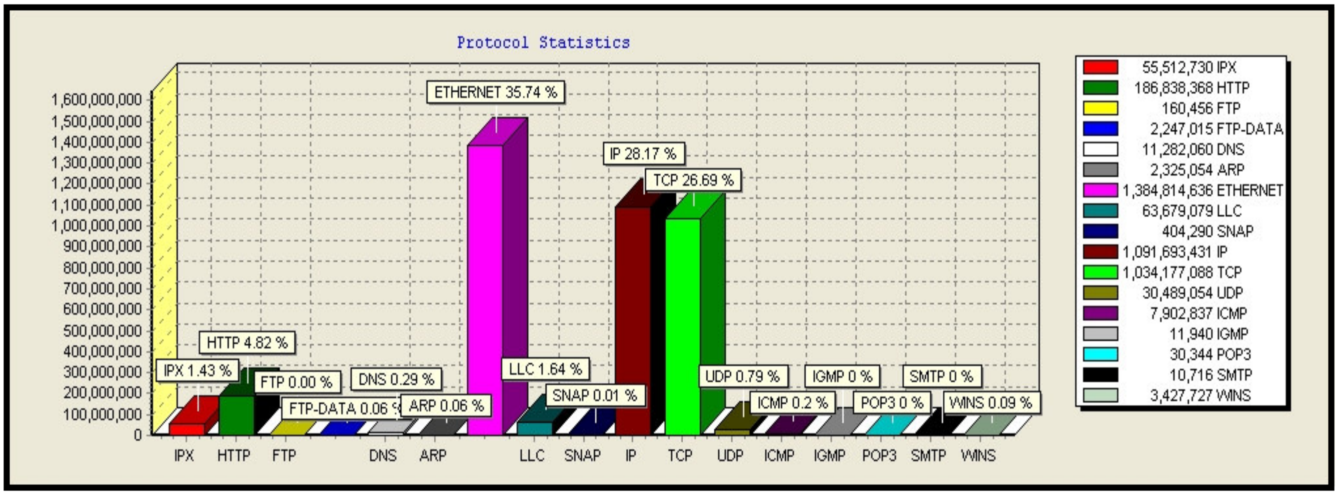

Figura 4.15: Gráfica general de protocolos generada por "Ultra Network Sniffer" para el equipo "SB2".

• Datos registrados en el Almacén, equipo "A1"

Reporte de Estadísticas Generado sobre 30/04/2004 a 01:50:37 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 01:29:58

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	63499	83.10
UDP	11198	14.65
ICMP	1712	2.24
IGMP	2	0.00

Tabla 4.38

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	9346693	27.29
FTP	0	0.00
POP3	2216	0.01
SMTP	0	0.00
Telnet	0	0.00
NNTP	0	0.00
NetBIOS	517248	1.51
HTTPS	358095	1.05
DNS	703114	2.05
Otros	23327356	68.10

Tabla 4.39

Reporte de Estadísticas Generado sobre 30/04/2004 a 02:20:37 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	56231	83.31
UDP	9589	14.21
ICMP	1674	2.48
IGMP	0	0

Tabla 4.40

Sub-protocolos IP

Sub-protocolo	Paquetes	Porcentaje
HTTP	13299	20.21
FTP	0	0.00
POP3	21	0.03
SMTP	0	0.00
Telnet	0	0.00
NNTP	0	0.00
NetBIOS	5292	8.04
HTTPS	222	0.34
DNS	3287	4.99
Otros	43699	66.39

Tabla 4.41

Tablas 4.38 – 4.41: Datos sobre los protocolos TCP/IP registrados en el equipo "A1"

Para los datos anteriores correspondientes a los registros de datos del equipo "A1", las figuras respectivas se muestran a continuación:

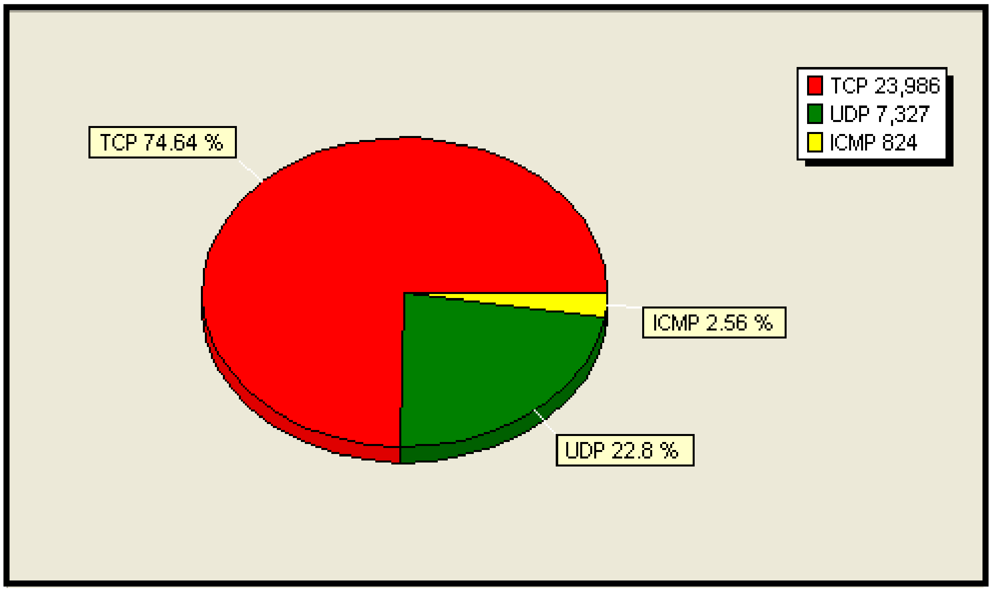

Figura 4.16: Protocolos registrados por "CommView" en el equipo "A1"

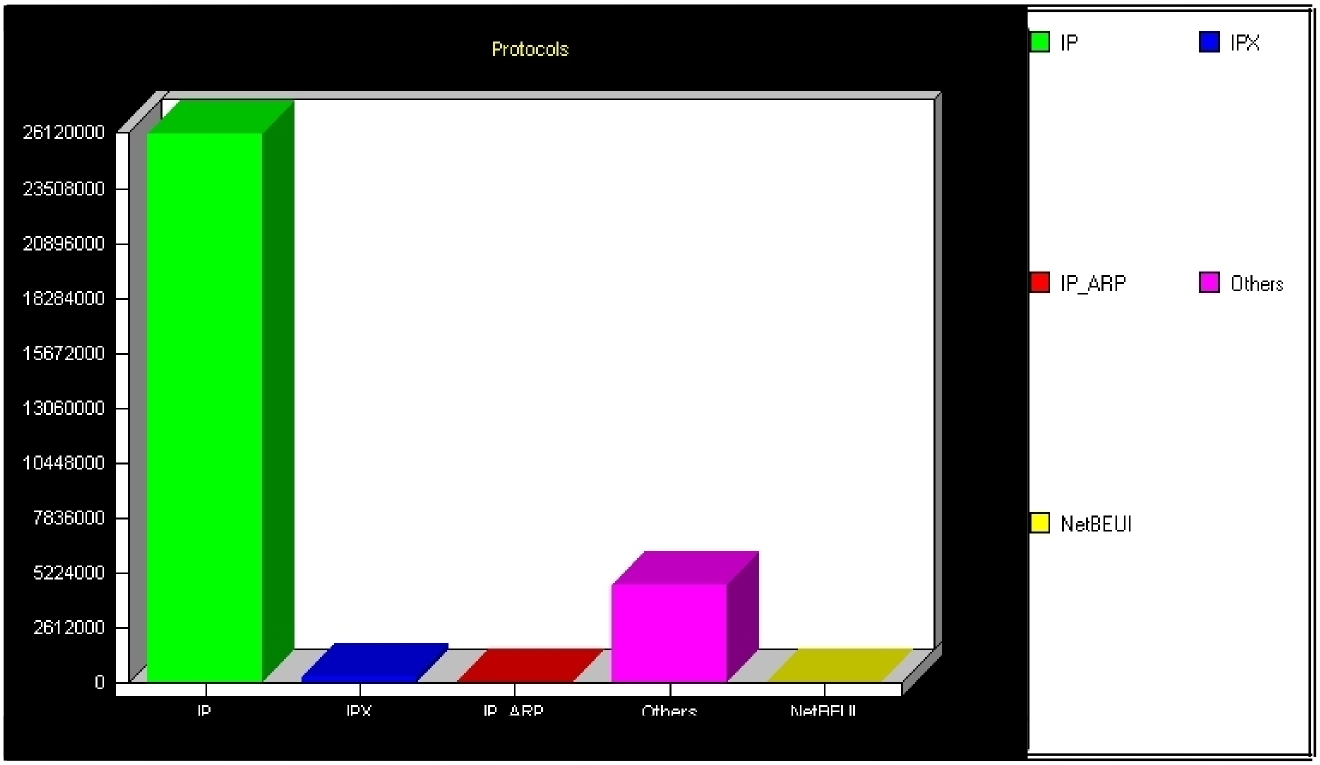

Figura 4.17: Protocolos encapsulados superiores al nivel MAC registrados en el equipo "A1 ".

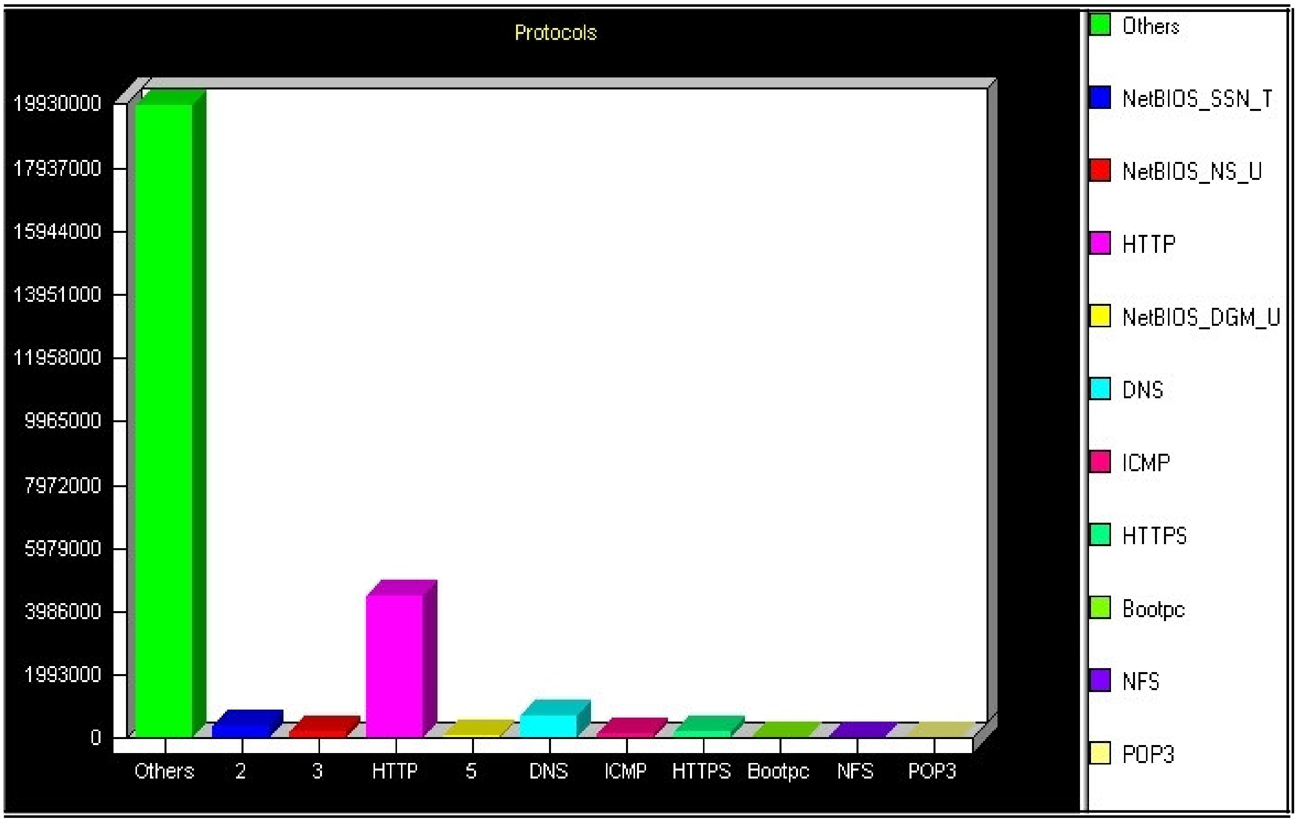

Figura 4.18: Protocolos de la pila TCP/IP registrados en el equipo "A1"

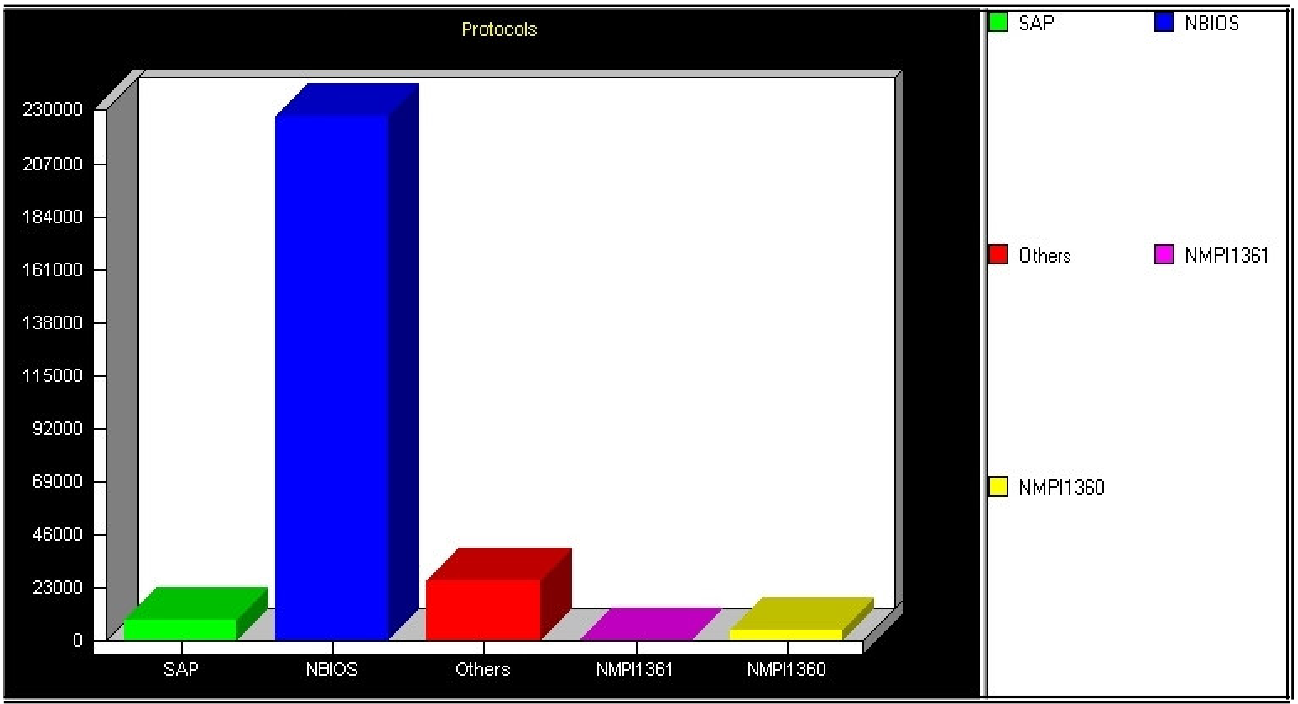

Figura 4.19: Protocolos del conjunto IPX registrados en el equipo "A1"

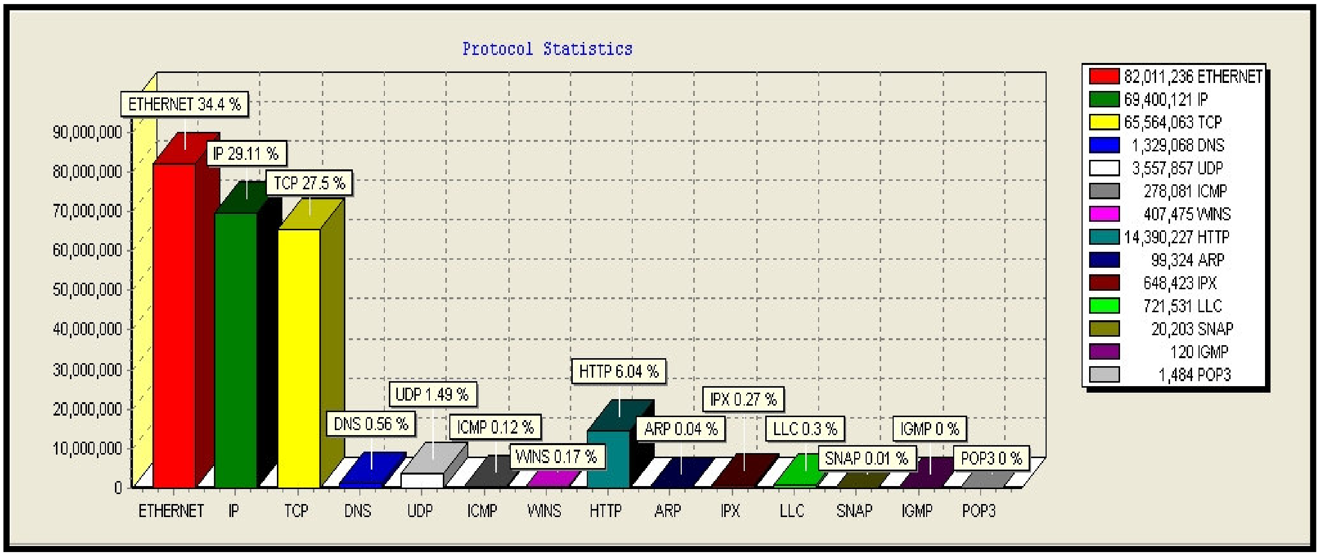

Figura 4.20: Gráfica general de protocolos generada por "Ultra Netwok Sniffer" para el equipo "A1".

- ## Datos registrados en S.S.E., equipo "S2"

Reporte de Estadísticas Generado sobre 29/04/2004 a 01:46:47 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	82337	72.39
UDP	20801	18.29
ICMP	2856	2.51
HBH-HEAD	7736	6.8
IGMP	4	0

Tabla 4.42

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	15549876	55.87
FTP	21994	0.08
POP3	3174	0.01
SMTP	0	0
Telnet	0	0
NetBIOS	1079471	3.88
HTTPS	811633	2.92
DNS	1804967	6.48
Otros	8563509	30.77

Tabla 4.43

Reporte de Estadísticas Generado sobre 29/04/2004 a 02:16:46 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

Protocolos IP

Protocolo	Paquetes	Porcentaje
TCP	70914	73.74
UDP	15184	15.79
ICMP	2243	2.33
HBH-HEAD	7817	8.13
IGMP	7	0.01

Tabla 4.44

Sub-protocolos IP

Sub-protocolo	Bytes	Porcentaje
HTTP	12734184	52.64
FTP	1158	0
POP3	2663	0.01
SMTP	0	0
Telnet	0	0
NetBIOS	1315625	5.44
HTTPS	486713	2.01
DNS	1085106	4.49
Otros	8564315	35.4

Tabla 4.45

Tablas 4.42 – 4.45: Datos sobre los protocolos TCP/IP registrados en el equipo "S2"

En este caso se cuenta con la siguiente información gráfica de acuerdo a los datos obtenidos en el equipo correspondiente:

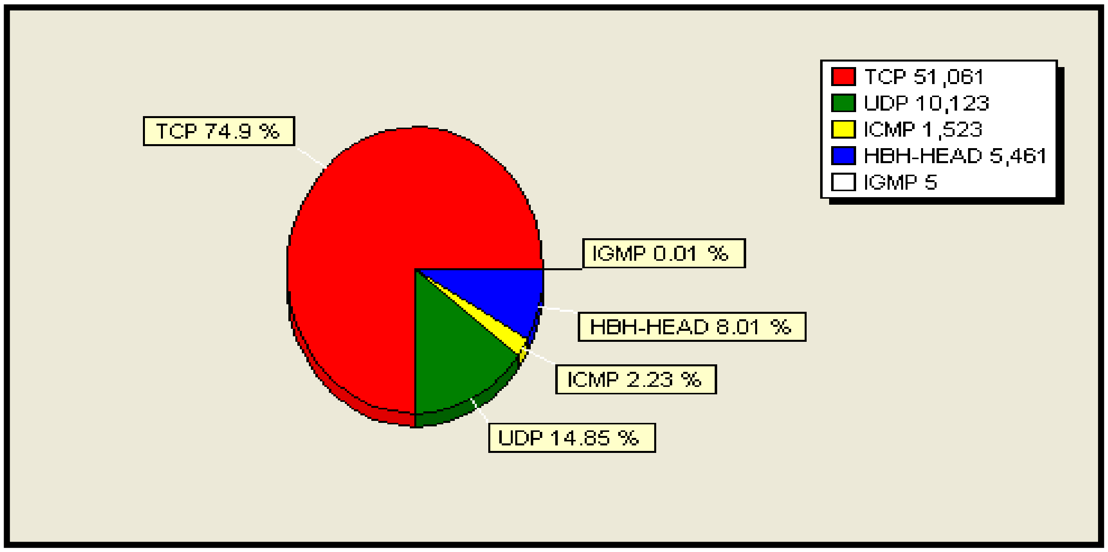

Figura 4.21: Protocolos registrados por "CommView" en el equipo "S2"

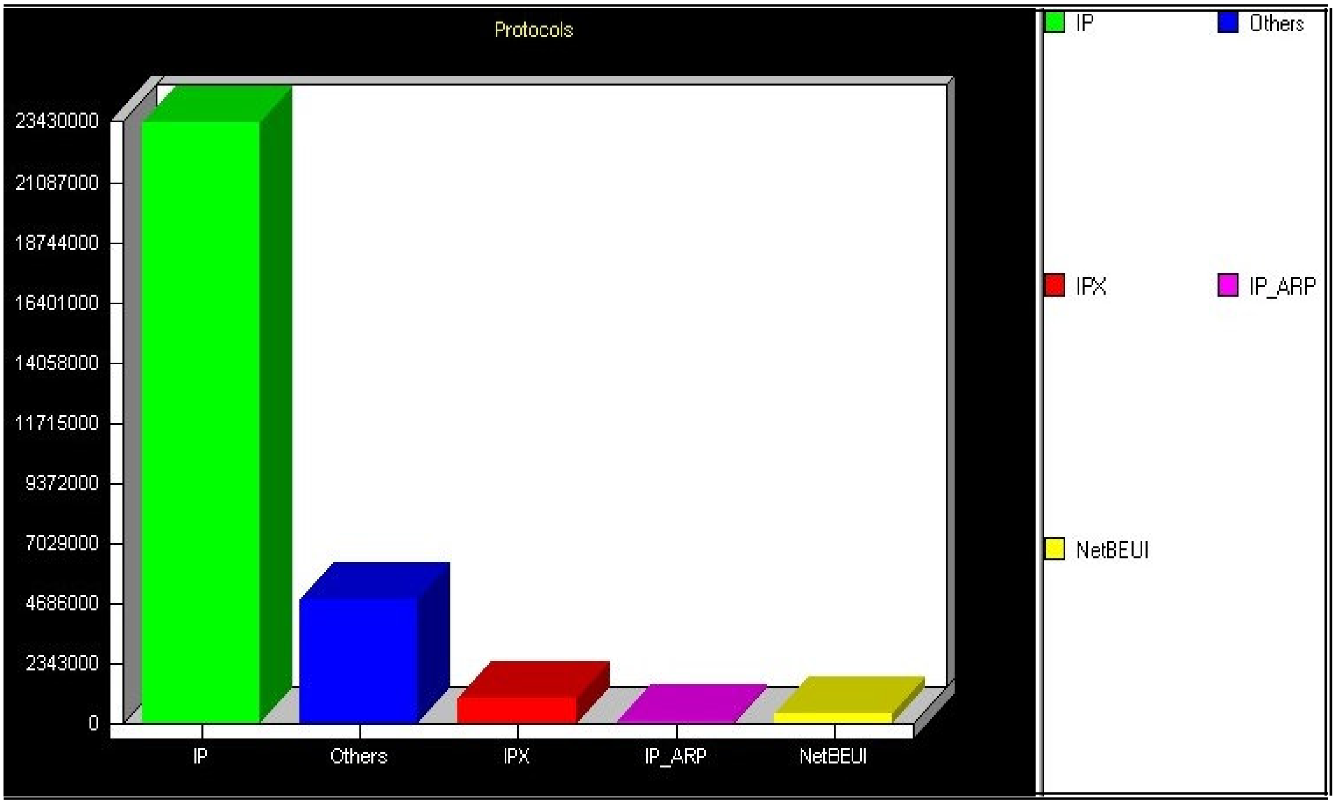

Figura 4.22: Protocolos encapsulados superiores al nivel MAC registrados en el equipo "S2".

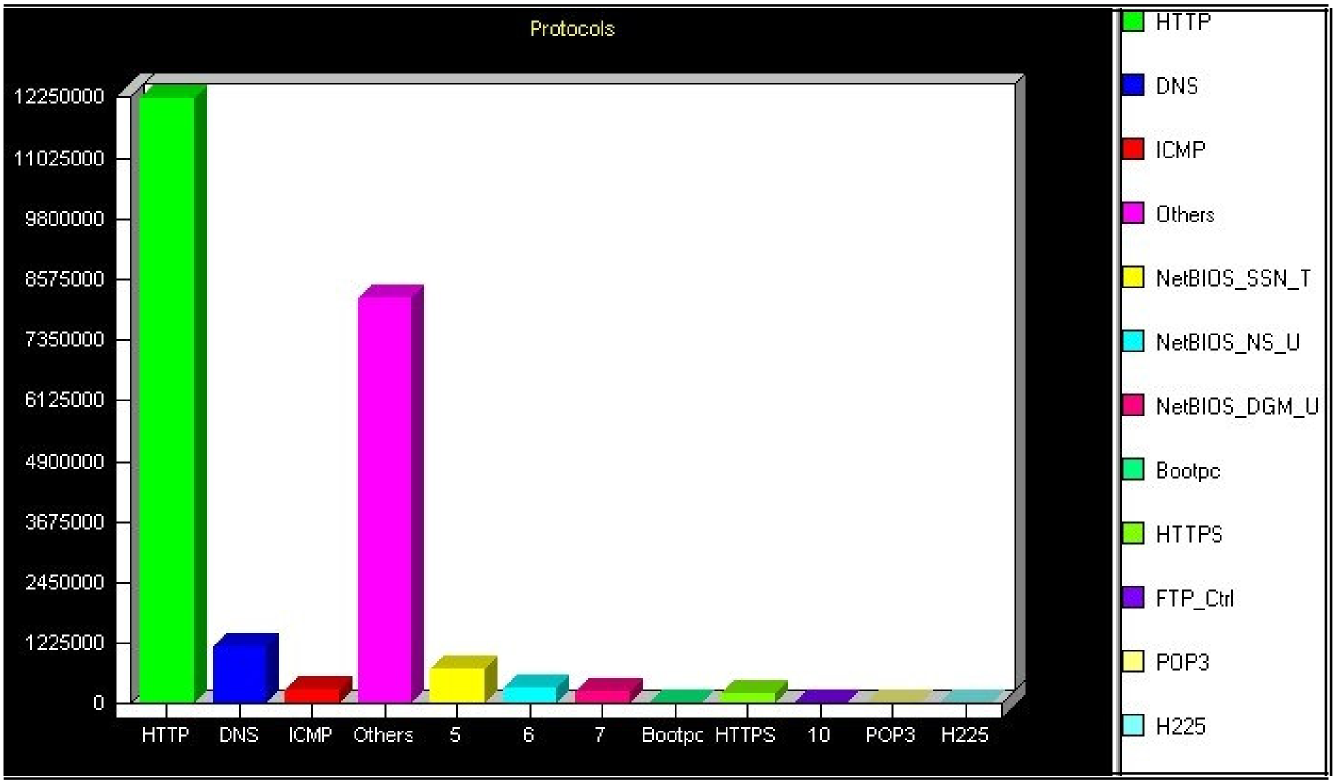

Figura 4.23: Protocolos de la pila TCP/IP registrados en el equipo "S2"

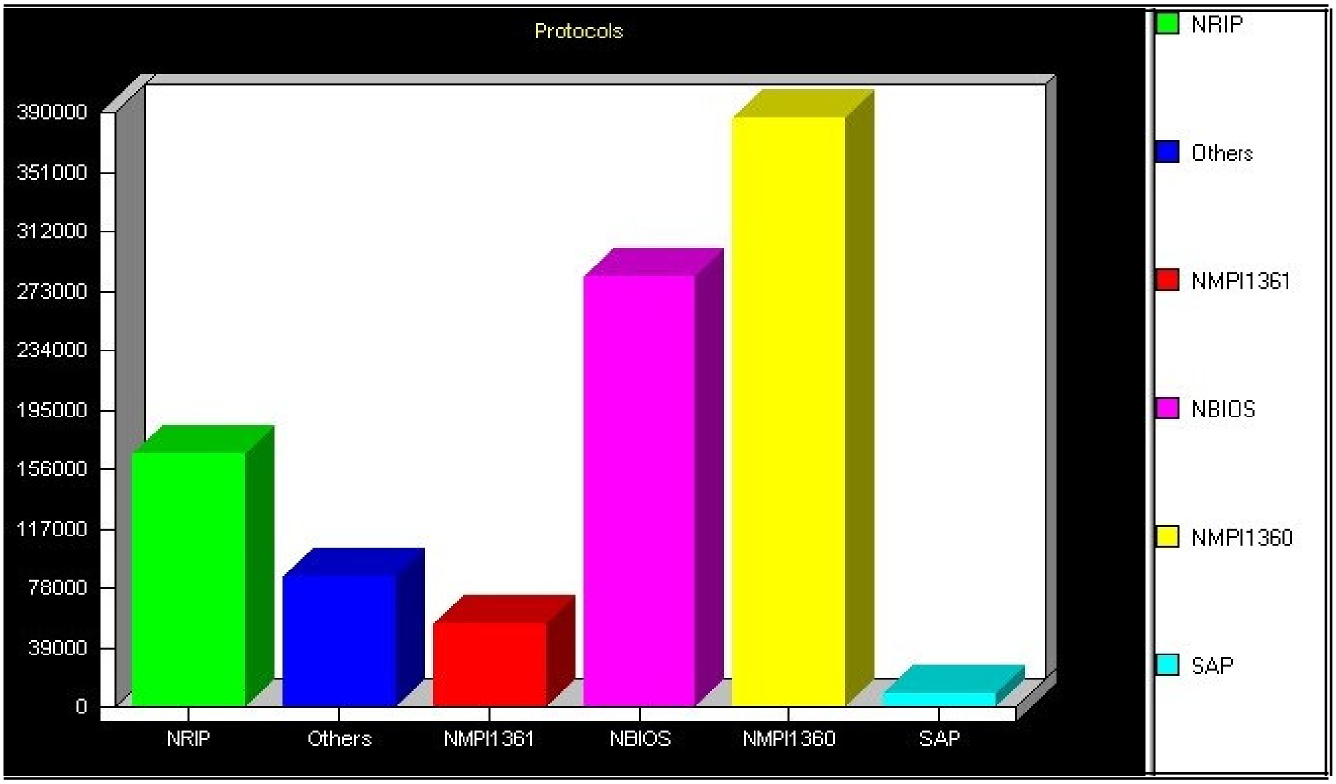

Figura 4.24: Protocolos del conjunto IPX registrados en el equipo "S2"

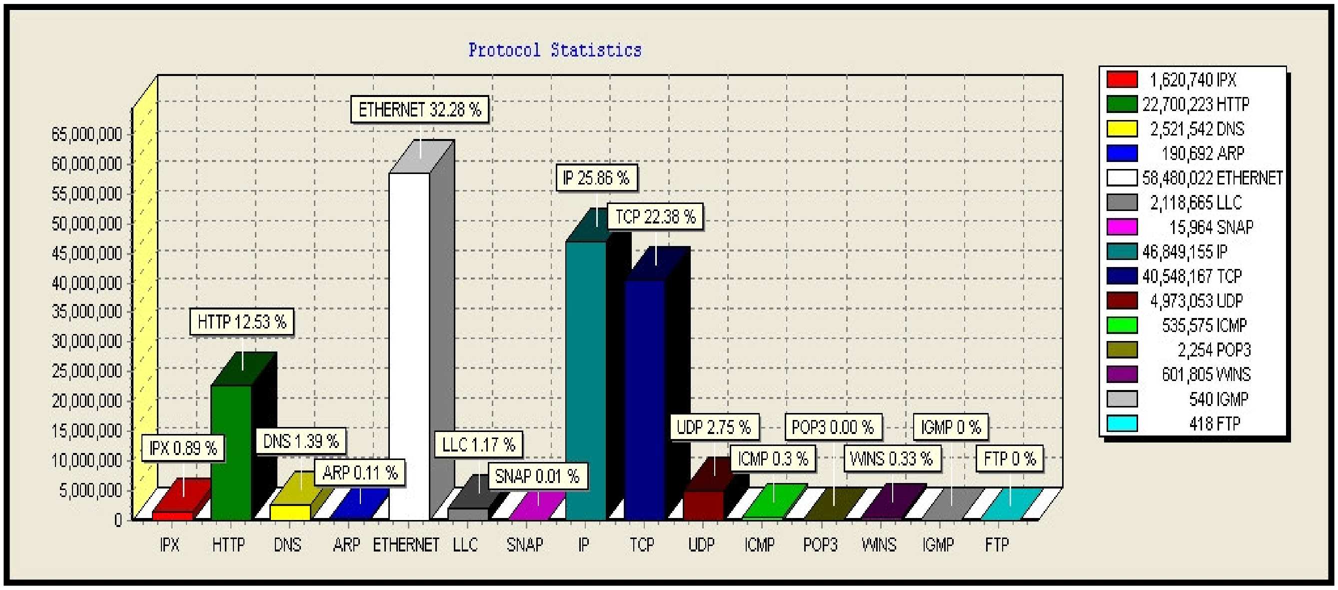

Figura 4.25: Gráfica general de protocolos generada por "Ultra Netwok Sniffer" para el equipo "S2".

De acuerdo a todos estos datos presentados tanto en tablas como gráficamente, analizando los resultados es posible realizar algunas observaciones. La primera de ellas es que, como se había mencionado anteriormente, el hecho de que uno de los programas no detecte ciertos protocolos no significa que éstos no existan en la operación de la red, de ahí la necesidad de utilizar más de un programa para el registro de información.

Los resultados muestran que en esta red además de la utilización de la pila TCP/IP también se hace uso del conjunto de protocolos de la categoría IPX, según se observa en todos los casos registrados mediante las gráficas de protocolos encapsulados en el nivel MAC proporcionadas por "Netasyst", además de las gráficas generales de protocolos desprendidas del programa "Ultra Network Sniffer" (UNS). De acuerdo a lo mostrado en esta información se hace constar que el protocolo IP predomina sobre IPX, teniendo versiones de protocolos (caso particular el de NetBIOS) que se presentan tanto en IP como en IPX.

Considerando los protocolos en general no es de extrañar, estudiando las gráficas de "UNS", que el protocolo que más domina en términos generales se trata del correspondiente al nivel MAC Ethernet, pues es en el que tiene que operar la red de acuerdo al tipo manejado para su caso y sobre el que se adecuan los protocolos restantes. También destaca, además del ya mencionado IP, el empleo del protocolo TCP, mismo que solamente en los registros tomados en el edificio "J" se ve superado por UDP. El nivel de utilización de TCP también concuerda con lo esperado, ya que como se sabe éste es empleado a su vez por los protocolos de aplicación para realizar las conexiones entre nodos necesarias para sus operaciones.

Finalmente, ya que se mencionan a los protocolos de la capa de aplicación, según lo visto en las imágenes se corrobora lo manifestado por los usuarios de la red, que mencionaron el uso en gran medida de consulta de correo e información general a través de páginas Web con el uso del protocolo HTTP, mismo que destaca en la gran mayoría de las gráficas sobre otros protocolos de este mismo nivel.

4.3.2.2 DESEMPEÑO DE LA RED.

El conocimiento del tipo de uso de la red así como de los protocolos que en ella se utilizan no es suficiente para establecer un panorama general del desempeño y la calidad de los servicios a los que accede un usuario. Para ello es necesario hacer uso de información adicional, también proporcionada por los programas analizadores de redes (“sniffers”), por lo que aún falta conocer parámetros como lo es el nivel de utilización, los errores que se generan en el flujo de datos, la cantidad de colisiones, así como la posible existencia de “cuellos de botella”. Estos son los puntos que se tratarán en las secciones siguientes, con el fin de completar el estudio de la situación actual de la red LAN del C.C.H. Vallejo, para posteriormente pasar al análisis de la información recaudada.

Errores y problemas generales.

Las colisiones excesivas es uno de los problemas comunes que podría encontrarse en una red que utiliza en su mayoría (o en la totalidad) concentradores como equipos de conexión, debido a la naturaleza del procedimiento de reenvío de tramas que realizan estos dispositivos. Por supuesto en las secciones en las que se emplean switches para la conexión de equipo este inconveniente no se hace presente.

Es sabido que una cantidad excesiva de colisiones tiene necesariamente como consecuencia una considerable retransmisión de tramas, que a ciertos niveles resulta indeseable, ya que provoca notorios retardos en la entrega de paquetes. Debido a estas circunstancias es necesario conocer el nivel de la presencia de colisiones en una red, con la finalidad de determinar si es debido a esta causa, cuando se presenta, un inadecuado desempeño de la red en uno o varios de sus segmentos.

Para los registros presentados enseguida, además de las colisiones detectadas se muestra la cantidad de tramas con errores que fueron registradas por el programa analizador, dato que también es conveniente conocer al considerarse como otra de las causas de retransmisión de paquetes. Las tablas que contienen estos registros son denominadas como “Tabla de Errores de NIC” por parte del programa “CommView” que es quien las genera. La traducción de la leyenda incluida en cada registro de dichas tablas es la siguiente:

- Type: Tipo (Dato registrado)
- Pkts: Paquetes
- Tx One Collision: Colisión con una trama (es decir, dos estaciones involucradas)
- Tx More Collisions: Colisión entre más de dos tramas.
- Tx Late Collisions: Colisiones tardías.
- Rx Frames w/Errors: Tramas recibidas con errores.
- Rx Frames w/o Errors: Tramas recibidas sin errores.
- Tx Frames w/Errors: Tramas enviadas con errores.
- Tx Frames w/o Errors: Tramas enviadas sin errores.

- **Datos generados en Siladin “B”, equipo “SB2“**

En este primer caso se presentan los datos de manera acumulada, es decir, para lo obtenidos en este equipo en particular, los registros de cada lapso se adicionaron a las cantidades previas de ocurrencia de eventos, dando como resultado un número total de los mismos durante el periodo de captura de información.

Las tablas mostradas corresponden a una selección en las que se tiene una mayor variación en las cantidades.

Reporte de Estadísticas
Generado sobre 29/04/2004 a 04:00:00 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 111,024

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	3
Tx More Collisions	6
Tx Late Collisions	0
Rx Frames w/Errors	516
Rx Frames w/o Errors	106740
Tx Frames w/Errors	0
Tx Frames w/o Errors	3768

Tabla 4.46

Reporte de Estadísticas
Generado sobre 29/04/2004 a 06:30:00 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 101,572

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	11
Tx More Collisions	7
Tx Late Collisions	0
Rx Frames w/Errors	2098
Rx Frames w/o Errors	440490
Tx Frames w/Errors	0
Tx Frames w/o Errors	3995

Tabla 4.47

Reporte de Estadísticas
Generado sobre 30/04/2004 a 12:00:00 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 65,487

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	16
Tx More Collisions	23
Tx Late Collisions	0
Rx Frames w/Errors	3101
Rx Frames w/o Errors	1226307
Tx Frames w/Errors	0
Tx Frames w/o Errors	11404

Tabla 4.48

Reporte de Estadísticas
Generado sobre 30/04/2004 a 11:00:00 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 412,872

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	32
Tx More Collisions	46
Tx Late Collisions	0
Rx Frames w/Errors	11826
Rx Frames w/o Errors	2905923
Tx Frames w/Errors	0
Tx Frames w/o Errors	18475

Tabla 4.49

Reporte de Estadísticas
Generado sobre 30/04/2004 a 11:30:00 a.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

General
Total de paquetes 148,712

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	39
Tx More Collisions	58
Tx Late Collisions	0
Rx Frames w/Errors	21876
Rx Frames w/o Errors	3058088
Tx Frames w/Errors	1
Tx Frames w/o Errors	19220

Tabla 4.50

Reporte de Estadísticas
Generado sobre 30/04/2004 a 12:00:00 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

General
Total de paquetes: 154, 236

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	46
Tx More Collisions	71
Tx Late Collisions	0
Rx Frames w/Errors	24481
Rx Frames w/o Errors	3208217
Tx Frames w/Errors	2
Tx Frames w/o Errors	23280

Tabla 4.51

Reporte de Estadísticas
Generado sobre 30/04/2004 a 12:37:13 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:07:13

General
Total de paquetes 15,996

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	47
Tx More Collisions	73
Tx Late Collisions	0
Rx Frames w/Errors	24685
Rx Frames w/o Errors	3317473
Tx Frames w/Errors	2
Tx Frames w/o Errors	24487

Tabla 4.52

Tablas 4.46 – 4.52 : Detección de colisiones y tramas con errores en el equipo “SB 2”

- **Datos generados en la Biblioteca, equipo “B2”**

En este y los casos subsecuentes, los registros presentados son los que mayor cantidad de colisiones y errores de tramas contienen dentro de un conjunto de datos obtenidos a distintas horas. Se presentan dicha selección con la finalidad de conocer el desempeño de la red bajo sus condiciones menos favorables.

Reporte de Estadísticas
Generado sobre 28/04/2004 a 02:11:08 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 150,640

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	16
Tx More Collisions	29
Tx Late Collisions	0
Rx Frames w/Errors	585
Rx Frames w/o Errors	140706
Tx Frames w/Errors	0
Tx Frames w/o Errors	9349

Tabla 4.53

Reporte de Estadísticas
Generado sobre 28/04/2004 a 02:41:08 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:50

General
Total de paquetes 152,711

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	114
Tx More Collisions	197
Tx Late Collisions	0
Rx Frames w/Errors	831
Rx Frames w/o Errors	144031
Tx Frames w/Errors	0
Tx Frames w/o Errors	7849

Tabla 4.54

Reporte de Estadísticas
Generado sobre 28/04/2004 a 04:06:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

General
Total de paquetes: 159,351

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	23
Tx More Collisions	43
Tx Late Collisions	0
Rx Frames w/Errors	397
Rx Frames w/o Errors	153389
Tx Frames w/Errors	0
Tx Frames w/o Errors	5565

Tabla 4.55

Reporte de Estadísticas
Generado sobre 28/04/2004 a 04:36:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

General
Total de paquetes 165,666

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	43
Tx More Collisions	86
Tx Late Collisions	0
Rx Frames w/Errors	749
Rx Frames w/o Errors	162758
Tx Frames w/Errors	0
Tx Frames w/o Errors	2159

Tabla 4.56

Reporte de Estadísticas
Generado sobre 28/04/2004 a 05:06:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:29:59

General
Total de paquetes 124,570

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	51
Tx More Collisions	101
Tx Late Collisions	0
Rx Frames w/Errors	944
Rx Frames w/o Errors	118051
Tx Frames w/Errors	0
Tx Frames w/o Errors	35575

Tabla 4.57

Reporte de Estadísticas
Generado sobre 28/04/2004 a 06:06:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 124,495

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	71
Tx More Collisions	127
Tx Late Collisions	3
Rx Frames w/Errors	1207
Rx Frames w/o Errors	119875
Tx Frames w/Errors	3
Tx Frames w/o Errors	43413

Tabla 4.58

Reporte de Estadísticas
Generado sobre 28/04/2004 a 07:06:21 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 13,828

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	71
Tx More Collisions	128
Tx Late Collisions	0
Rx Frames w/Errors	1207
Rx Frames w/o Errors	11174
Tx Frames w/Errors	3
Tx Frames w/o Errors	1447

Tabla 4.59

Tablas 4.53 – 4.59: Detección de colisiones y tramas con errores en el equipo "B 2"

- **Datos generados en el Almacén, equipo "A1".**

Reporte de Estadísticas
Generado sobre 30/04/2004 a 01:50:37 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 01:29:58

General
Total de paquetes 83,751

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	2
Tx More Collisions	7
Tx Late Collisions	0
Rx Frames w/Errors	118
Rx Frames w/o Errors	80973
Tx Frames w/Errors	0
Tx Frames w/o Errors	2660

Tabla 4.60

Reporte de Estadísticas
Generado sobre 30/04/2004 a 02:20:37 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 74,848

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	3
Tx More Collisions	10
Tx Late Collisions	0
Rx Frames w/Errors	251
Rx Frames w/o Errors	73122
Tx Frames w/Errors	0
Tx Frames w/o Errors	1475

Tabla 4.61

Reporte de Estadísticas
Generado sobre 30/04/2004 a 01:50:37 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 01:29:58

General
Total de paquetes 85,435

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	5
Tx More Collisions	12
Tx Late Collisions	0
Rx Frames w/Errors	123
Rx Frames w/o Errors	82877
Tx Frames w/Errors	0
Tx Frames w/o Errors	2435

Tabla 4.62

Reporte de Estadísticas
Generado sobre 30/04/2004 a 01:50:37 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 01:29:58

General
Total de paquetes 81,852

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	9
Tx More Collisions	15
Tx Late Collisions	0
Rx Frames w/Errors	112
Rx Frames w/o Errors	79695
Tx Frames w/Errors	0
Tx Frames w/o Errors	2045

Tabla 4.63

Tablas 4.60 – 4.63: Detección de colisiones y tramas con errores en el equipo "A1"

- **Datos generados en el Edificio “J”, equipo “J4”**

Reporte de Estadísticas
Generado sobre 19/04/2004 a 08:46:42 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 23,445

Tabla de errores de NIC

Type	Pkts
Tx One Collision	0
Tx More Collisions	0
Tx Late Collisions	0
Rx Frames w/Errors	6
Rx Frames w/o Errors	22025
Tx Frames w/Errors	0
Tx Frames w/o Errors	1414

Tabla 4.64

Reporte de Estadísticas
Generado sobre 19/04/2004 a 10:50:30 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 30,793

Tabla de errores de NIC

Type	Pkts
Tx One Collision	0
Tx More Collisions	0
Tx Late Collisions	0
Rx Frames w/Errors	2
Rx Frames w/o Errors	29227
Tx Frames w/Errors	0
Tx Frames w/o Errors	1564

Tabla 4.65

Reporte de Estadísticas
Generado sobre 19/04/2004 a 02:46:40 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 29,918

Tabla de errores de NIC

Type	Pkts
Tx One Collision	0
Tx More Collisions	0
Tx Late Collisions	0
Rx Frames w/Errors	1
Rx Frames w/o Errors	27593
Tx Frames w/Errors	0
Tx Frames w/o Errors	2324

Tabla 4.66

Reporte de Estadísticas
Generado sobre 21/04/2004 a 05:50:32 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 31, 276

Tabla de errores de NIC

Type	Pkts
Tx One Collision	0
Tx More Collisions	0
Tx Late Collisions	0
Rx Frames w/Errors	4
Rx Frames w/o Errors	29422
Tx Frames w/Errors	1
Tx Frames w/o Errors	1849

Tabla 4.67

Reporte de Estadísticas
Generado sobre 20/04/2004 a 08:30:27 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 31, 165

Tabla de errores de NIC

Type	Pkts
Tx One Collision	0
Tx More Collisions	0
Tx Late Collisions	0
Rx Frames w/Errors	3
Rx Frames w/o Errors	29087
Tx Frames w/Errors	1
Tx Frames w/o Errors	2074

Tabla 4.68

Tablas 4.64 - 4.68: Detección de colisiones y tramas con errores en el equipo "J 4"

- **Datos generados en el edificio de la S.S.E, equipo "S2"**

Reporte de Estadísticas
Generado sobre 29/04/2004 a 09:46:47 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 127,063

Tabla de Errores de NIC

Type	Pkts
Tx One Collision	9
Tx More Collisions	12
Tx Late Collisions	0
Rx Frames w/Errors	253
Rx Frames w/o Errors	120110
Tx Frames w/Errors	0
Tx Frames w/o Errors	6700

Tabla 4.69

Reporte de Estadísticas
Generado sobre 29/04/2004 a 12:16:46 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 110,695

Tabla de errores de NIC

Type	Pkts
Tx One Collision	12
Tx More Collisions	23
Tx Late Collisions	0
Rx Frames w/Errors	260
Rx Frames w/o Errors	107945
Tx Frames w/Errors	0
Tx Frames w/o Errors	2490

Tabla 4.70

Reporte de Estadísticas
Generado sobre 29/04/2004 a 4:16:46 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 123,258

Tabla de errores de NIC

Type	Pkts
Tx One Collision	10
Tx More Collisions	12
Tx Late Collisions	1
Rx Frames w/Errors	185
Rx Frames w/o Errors	119953
Tx Frames w/Errors	0
Tx Frames w/o Errors	3120

Tabla 4.71

Reporte de Estadísticas
Generado sobre 29/04/2004 a 05:16:46 p.m. por CommView. Tiempo de captura desde el último reinicio (hh:mm:ss): 00:30:00

General
Total de paquetes 131,652

Tabla de errores de NIC

Type	Pkts
Tx One Collision	12
Tx More Collisions	23
Tx Late Collisions	0
Rx Frames w/Errors	284
Rx Frames w/o Errors	128110
Tx Frames w/Errors	0
Tx Frames w/o Errors	3258

Tabla 4.72

Tablas 4.69 – 4.72: Detección de colisiones y tramas con errores en el equipo “S2“

De los equipos analizados se tiene que el registro de colisiones, considerando una totalidad entre todas las categorías de las mismas, no se considera como grave en ninguno de los casos, ya que la cantidad de eventos no es comparable con el total de paquetes circulados en los periodos de toma de datos. El caso contrario implicaría que muchos de los paquetes detectados se hubieran tratado de simples reenvíos en lugar de tramas nuevas a entregar. Se tendría el mismo caso para los paquetes que contienen errores, ya que en esta situación el nodo receptor también requiere de una retransmisión.

El caso mas notable, en cuanto a colisiones, se tiene en el equipo “B2” de la Biblioteca, donde uno de los registros presenta 114 colisiones entre dos tramas y 197 entre más de dos. El programa CommView no especifica para este último dato la cantidad exacta de paquetes entre los que se presenta el incidente; a pesar de esto, si se compara el total de paquetes para este caso en específico que es de 152,711, aún teniéndose una cantidad considerable de retransmisiones debidas a estas colisiones, no se volvería una cantidad de reenvíos muy significativa respecto al total de paquetes enviados.

Tomando los datos de este ejemplo en particular, se sabe que debido a las 114 colisiones entre dos estaciones se debe hacer el doble de retransmisiones, ya que por cada colisión están involucrados dos nodos, de tal forma que es necesario realizar 228 retransmisiones debidas a este tipo de colisiones. Además considerando que para las 197 colisiones entre más de dos estaciones se tuvieran 24 nodos involucrados en cada caso, de acuerdo al numero total de puertos del equipo (lo cual es poco probable), se requerirían 4728 reenvíos como consecuencia de esta última situación, teniendo así un total de 4956 retransmisiones debidas al total de las colisiones, lo que implicaría que se hubieran realizado 147,755 envíos normales.

Ahora bien, para este mismo caso existe un registro de 831 tramas con errores, lo que sumado a las retransmisiones deducidas anteriormente daría una cantidad de 5609 reenvíos totales, para tener así 147,102 transmisiones normales. Este dato implica que menos del 4% de las emisiones de datos en este registro se deben a reenvíos. Analizando el resto de los casos se visualizan situaciones parecidas.

En el concentrador principal no se tomaron datos como los analizados en los casos anteriores, debido a la imposibilidad de realizar una conexión directa en él, ya que sólo cuenta con puertos para conexión de fibra óptica. Sin embargo este concentrador cuenta con un indicador que determina el momento de una colisión en el equipo, de tal forma que se logró determinar que en promedio se presentan 28 colisiones por minuto, que traducido al mismo periodo de los registros del resto de los equipos (30 minutos) se tienen entonces 840 colisiones en promedio para un periodo de 30 minutos en el concentrador principal. Por la misma situación de la imposibilidad de conexión, no se cuenta con un registro de la cantidad de paquetes circulados en este equipo, pero considerando la cantidad de colisiones respecto al número de paquetes detectados en los otros concentradores, parece tampoco tenerse en este caso un problema de retransmisiones locales, al menos con la cantidad de usuarios actuales de la red.

En otra categoría aparecen las retransmisiones incluidas en las sesiones del protocolo TCP, mismas que se presentan cuando los paquetes de confirmación de este protocolo no son entregados. Haciendo una revisión de los datos generados tanto por el programa “Netasyst” como por “Agilent Advisor”, se observa que, aún cuando dichos programas muestran además otras categorías de problemas, éste es uno de los grandes inconvenientes que de manera más frecuente afecta a la red.

Antes de continuar con la presentación de datos, es necesario hacer la observación de que el grupo de direcciones IP asignadas para la red de Vallejo corresponde al último octeto del segmento 132.248.88.0, por lo que se dispone de la direcciones 132.248.88.0 a la 132.248.88.255. Esta información permitirá conocer cuáles de los nodos presentes en los registros pertenecen a la red analizada, para tener claro la dirección de la comunicación cuando se trata de conexiones con nodos externos. La tabla 4.73 corresponde a una selección de diversas capturas de datos obtenidos mediante “Netasyst” y contiene información sobre los problemas frecuentes y la duración de los mismos.

First Time	Duration	Description	Object
27/04/04 12:13	5m 30s 43ms	Too Many Retransmissions	TCP: 132.248.88.127 - 213.4.130.210 Port 1471 - 80
27/04/04 17:16	4m 18s 239ms	Too Many Retransmissions	TCP: 64.233.167.99 - 132.248.88.145 Port 80 - 1320
28/04/04 14:02	4m 15s 474ms	Too Many Retransmissions	TCP: 132.248.88.11 - 200.77.25.15 Port 3371 – 3637
28/04/04 18:14	<1ms	Non-Responsive Station	TCP: 132.248.88.113 - 207.68.162.250 Port 1568 - 80
29/04/04 11:36	<1ms	Non-Responsive Station	TCP: 132.248.88.113 - 207.68.162.250 Port 1568 - 80
29/04/04 19:23	1m 2s 950ms	Too Many Retransmissions	TCP: 132.248.88.157 - 216.239.37.104 Port 1454 - 80
29/04/04 17:14	2m 26s 436ms	Too Many Retransmissions	TCP: 66.35.229.172 - 132.248.88.13 Port 80 - 1317
29/04/04 17:14	2m 10s 408ms	Too Many Retransmissions	TCP: 132.248.88.157 - 216.239.37.104 Port 1453 - 80
30/04/04 10:35	5m 58s 638ms	Too Many Retransmissions	TCP: 63.211.153.87 - 132.248.88.170 Port 80 - 3208
30/04/04 14:22	7m 25s 311ms	Too Many Retransmissions	TCP: 64.152.73.143 - 132.248.88.9 Port 80 - 1190

Tabla 4.73: Problemas detectados por “Netasyst, donde: First Time – Inicio del evento, Duration – Duración, Description – Descripción (Acontecimiento), Objet – Objeto (Conexión involucrada). Para el contenido: Too many Retransmisions – Demasiadas retransmisiones, Non-responsive station - Estación sin respuesta, Port – Puerto.

El resto de los datos generados muestra la misma tendencia presentada, donde las retransmisiones prevalecen sobre la indicación de estaciones sin respuesta y otros acontecimientos. No es posible mostrar todos los datos debido a la extensión de los mismos, ya el programa analiza las situaciones ocurridas con cada conexión hecha por todo nodo perteneciente a la red.

Para contar con una visión general de la detección de problemas respecto al protocolo TCP, y tener más clara la predominancia de retransmisiones sobre otros inconvenientes, se hará uso de las estadísticas generadas por "Agilent Advisor", programa analizador que muestra un resumen con las respectivas cantidades referentes a la ocurrencia de eventos detectados. La información, que corresponde en cada caso a un periodo de 30 minutos, es presentada en el contenido de las figuras 4.26 a, 4.26 b y 4.26 c.

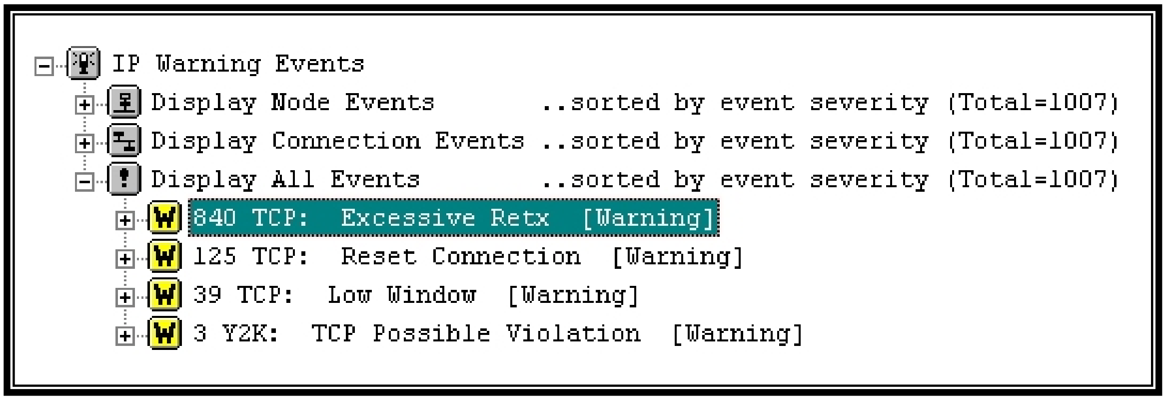

Figura 4.26 a

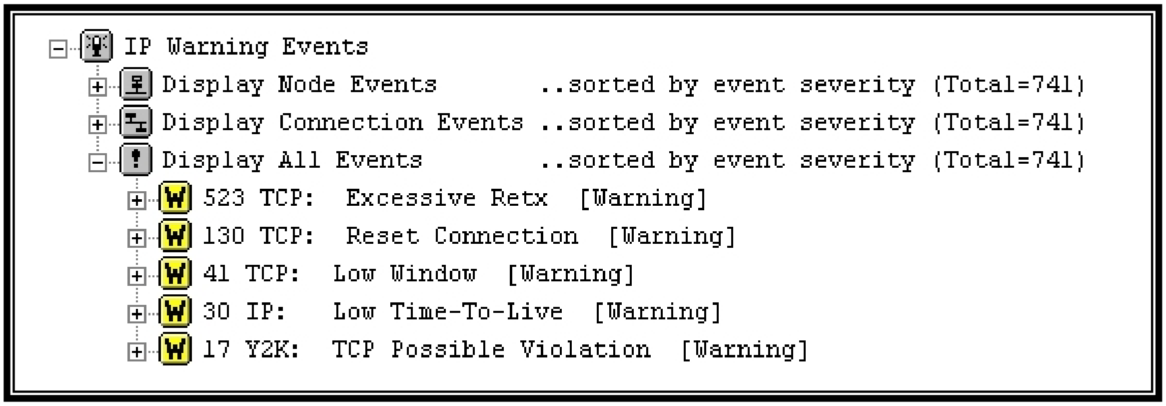

Figura 4.26 b

Ahora bien, con el fin de conocer más a fondo la situación que prevalece como consecuencia de la presencia de estos eventos, será necesario analizar casos en particular de los que se presentan en las estadísticas previamente mostradas. Las figuras 4.27a , 4.27b y 4.27c contienen algunos estos ejemplos detectados de retransmisiones dentro de las sesiones TCP:

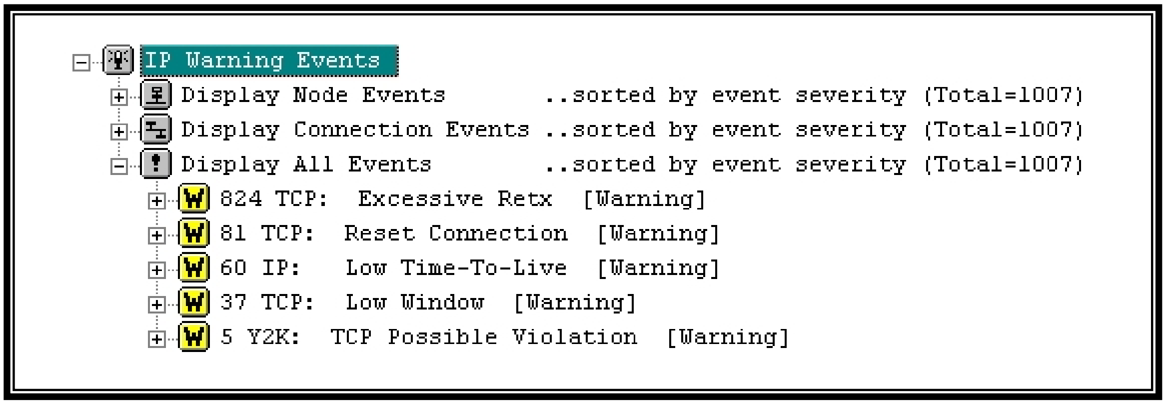

Figura 4.26 c

Figuras 4.26 a – 4.26 c: Registros de eventos de conexión correspondientes a horas distintas de tres diferentes días, donde IP Warning Events – Eventos de advertencia IP, Excesive Retx – Retransmisiones Excesivas, Reset Connection - Reinicio o de Conexión, Low Time to Live - Parámetro IP de tiempo de vida muy bajo, Low Windows – Ventana muy pequeña, TCP Possible Violation – Posible violación TCP

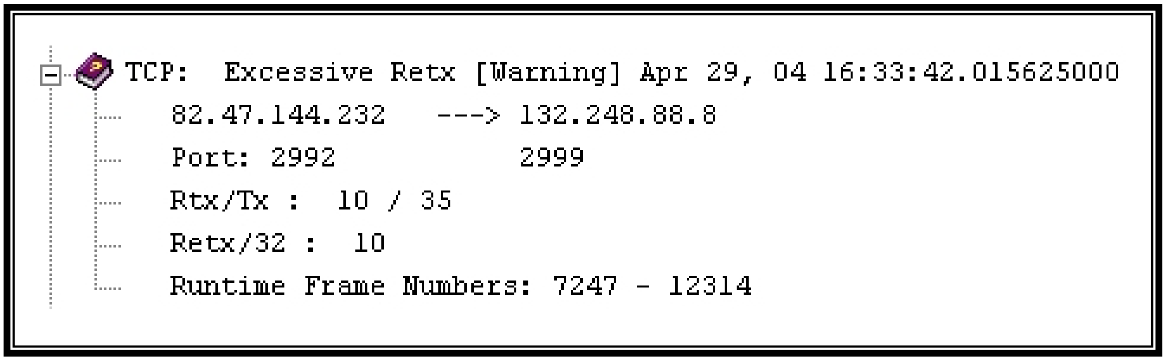

Figura 4.27 a

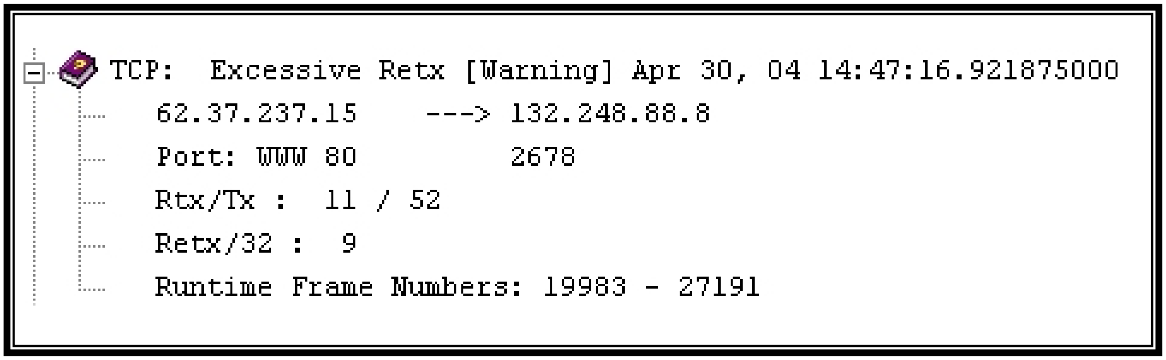

Figura 4.27 b

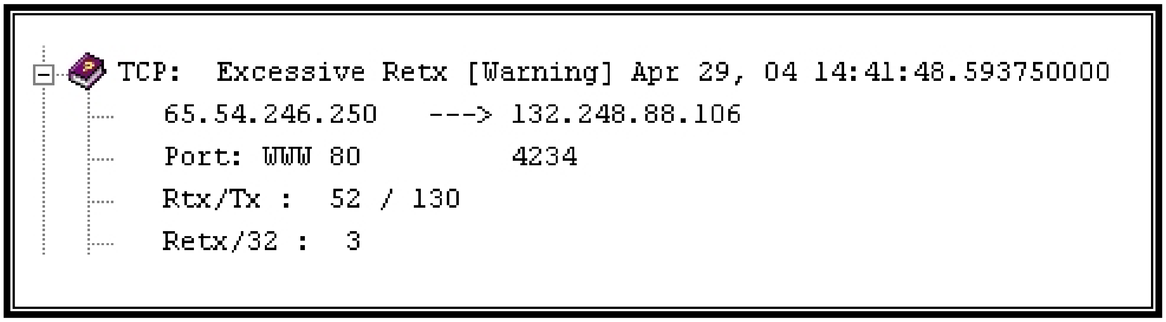

Figura 4.27 c

Figuras 4.27 a – 4.27 c: Ejemplos de casos de retransmisiones excesivas, donde: Port – Puertos involucrados, Rtx/Tx – Relación entre retransmisiones y envíos totales.

Otros de los casos referentes a retransmisiones se declaran en la tabla 4.74 con sus respectivas estadísticas. El contenido de la tabla corresponde a un número restringido de datos representativos del comportamiento general de las sesiones TCP.

Net Station 1	Net Station 2	Protocol	Frames	Bytes	Quantity of Diag/Symp	**Diag/Symp**
[64.152.73.153]	ADMINISTRATIVA ([132.248.88.9])	TCP	31	10896	11	Too Many Retransmissions
[64.233.167.99]	BIOLOGA ([132.248.88.62])	TCP	30	11407	16	Too Many Retransmissions
UNAM-0BRDMYZA3T ([132.248.18.110])	DOCENTE2 ([132.248.88.8])	TCP	27	2268	16	Too Many Retransmissions
[4.152.73.153]	ESTUDIANTILES ([132.248.88.119])	TCP	13	2198	5	Too Many Retransmissions
[63.215.198.186]	PARTICULAR ([132.248.88.5])	TCP	13	1454	6	Too Many Retransmissions
ACADEMICA ([132.248.88.4])	[207.46.134.92]	TCP	16	1424	12	Too Many Retransmissions
GENERAL ([132.248.88.3])	[209.247.153.137]	TCP	22	2688	13	Too Many Retransmissions
ALMACEN03 ([132.248.88.111])	[216.91.187.195]	TCP	16	1694	10	Too Many Retransmissions
[130.111.151.127]	LIBRERIA ([132.248.88.112])	TCP	22	2337	12	Too Many Retransmissions
[132.248.88.10]	www.gocyberlink.com ([216.136.183.10]) TCP	TCP	13	3348	9	Too Many Retransmissions
[63.215.198.185]	SISTEMAS6 ([132.248.88.106])	TCP	25	9454	22	Too Many Retransmissions

Tabla 4.74: Ejemplos representativos de casos de retransmisiones TCP, donde: Net Station 1 – Estación de red 1. Net Station 2 – Estación de red 2, Protocol – Protocolo, Frmaes – Tramas, Quantity of Diag/Symp – Cantidad de Diagnósticos/Síntoma, Diag/Symp – Diagnóstico/Síntoma.

Se observa para los ejemplos anteriores que siempre uno de los nodos involucrados es exterior a la red LAN del C.C.H. Vallejo, lo cual no implica que no existan registros similares para conexiones internas. La razón por la cual no se seleccionaron estadísticas que consideren sesiones entre dos nodos locales, es debido a que la cantidad de estos casos no es comparable al número de situaciones del tipo de las contenidas en las tablas e imágenes anteriores, motivo por el cual este tipo de sesiones con nodos externos representaron una mejor muestra para realizar el estudio correspondiente.

Entrando pues al análisis, es notorio que no se presenta la misma situación que para las retransmisiones ocasionadas por colisiones, donde se tenía que el porcentaje de reenvíos no era muy significativo respecto al total de las transmisiones. En cambio para las sesiones TCP, de acuerdo a los registros seleccionados, se observa que en los casos más graves la cantidad de retransmisiones representa más de la mitad del número total de tramas enviadas, lo que significa que una transacción de información mediante varios paquetes en una sesión TCP, en las circunstancias más adversas, está requiriendo el doble del tiempo normal para completarse, situación que a diferencia de otro tipo de dificultades, ésta si es detectada plenamente por los usuarios.

Aún cuando no siempre se tiene este grado de reenvíos, lo cierto es que de acuerdo a una cantidad mayor de registros con los que se cuenta, los presentados no se tratan de casos aislados. Es por ello que considerando la cantidad de situaciones de reenvíos excesivos registrados, aunado a que este protocolo es de los más usados en la red por encima de su paralelo del tipo “no orientado a conexión” UDP, se tiene entonces aquí una de las mayores problemáticas que afectan el desempeño adecuado de la red.

Disponibilidad y nivel de utilización.

El grado de disponibilidad de los servicios ofrecidos por una red dependerá necesariamente del nivel de utilización, ya que éste es quien dicta la demanda que se haga del ancho de banda disponible, ya sea interno (en la red LAN) o para acceso a Internet (enlace WAN).

Bajo las circunstancias en las que exista un ancho de banda saturado la facilidad para el flujo de datos se verá disminuida, en primer instancia por las propias restricciones debidas a las características de los medios de transmisión y los equipos de conexión, y en segundo término como consecuencia del incremento de los problemas citados en las secciones anteriores.

El nivel de utilización no sólo tiene que ver con la intensidad de tareas de los usuarios, sino además con la forma de comunicarse de ciertos protocolos, ya que un descontrol en la interacción mediante mensajes de difusión general o multidifusión, como caso extremo, puede llegar a ocasionar una saturación de los medios de transmisión.

Será entonces el nivel de utilización el siguiente punto a analizar para la red en cuestión. Para ello es necesario conocer datos sobre la cantidad de paquetes circulados por la red, determinando cuántos de ellos son del tipo de difusión y en general verificar la carga del ancho de banda. Estos datos se encuentran contenidos en las tablas siguientes, mismos que se analizaran en cada uno de los casos.

Promedio de paquetes por seg.	61
Promedio de bytes por seg.	19996
Total de paquetes	110422
Total bytes	35988978

Tabla 4.75

Dirección	Pqts Rec.	Bytes Rec.
Broadcast	11263	6509278
Multicast	723	114649

Tabla 4.76

Según los datos contenidos en los registros anteriores se tiene un total de 110,422 paquetes, de los cuales 11,263 son de difusión general (“broadcast”) y 723 de multidifusión (“multicast”). Adicionando las cantidades de los dos tipos de mensajes de difusión da un total de 111,145, es decir poco más del 10% del total de paquetes circulados. En cuanto a bytes se refiere, este tipo de mensajes ocupan un total de 18.4% del flujo de datos.

Por otro lado, el promedio de bytes por segundo indica una cantidad de 19,996, que traducido a bits representa un flujo de 160 kbps. Considerando que la máxima velocidad de transferencia para la red LAN con la que se cuenta ahora es de 10 Mbps, estos 160 kbps representan una utilización del ancho de banda interno de 1.6%. Antes de obtener conclusiones es necesario corroborar y comparar con otras muestras:

General

Promedio de paquetes por seg.	85
Promedio de bytes por seg.	22461
Total de paquetes	152711
Total bytes	40443761

Tabla 4.77

Dirección	Pqts Rec.	Bytes Rec.
Broadcast	8372	6154967
Multicast	416	56198

Tabla 4.78

En este otro registro se presentan 152,711 paquetes totales, y una cantidad de 8788 de mensajes de difusión, que representan el 5.75%. En cuestión de bytes para difusión general y multidifusión existe un total de 6,211,165, siendo éstos un 15.35%. Se tiene entonces que desde este punto de vista la cantidad de información de difusión es más elevada de lo que podría considerarse al analizar simplemente los paquetes.

La ocupación del ancho de banda está dada por los 22,461 bytes por segundo en promedio, de tal forma que en su equivalente en bits existe un flujo de 180 kbps, es decir 1.8% del total del ancho de banda.

Un tercer registro de datos es el mostrado enseguida:

General

Promedio de paquetes por seg.	81
Promedio de bytes por seg.	23095
Total de paquetes	145519
Total bytes	41570100

Tabla 4.79

Dirección	Pqts Rec.	Bytes Rec.
Broadcast	8933	6190284
Multicast	1035	161228

Tabla 4.80

Para este caso la situación no es muy diferente de las anteriores, al tener 6,351,512 de bytes de difusión, representando un 15.3%. El ancho de banda ocupado es del 1.84%.

Solamente en uno de los sectores de la red, hacia la zona que comprende el edificio “J”, se detectaron lecturas distintas al resto. De acuerdo a las tablas correspondientes, se tiene una disminución en la lectura de paquetes y por tanto en el promedio de bytes por segundo. Por el contrario se incrementa el uso de mensajes de difusión para la comunicación entre nodos:

General

Promedio de paquetes por seg.	9
Promedio de bytes por seg.	3860
Total de paquetes	16050
Total bytes	6948112

Tabla 4.81

Dirección	Pqts Rec.	Bytes Rec.
Broadcast	9150	6157247
Multicast	1194	137780

Tabla 4.82

Tablas 4.75, 4.77, 4.79 y 4.81: Registro de paquetes y bytes circulados en un periodo de 30 minutos para cada caso.
Tablas 4.76, 4.78, 4.80 y 4.82: Registro de mensajes de difusión detectados en la red para un lapso de 30 minutos en cada situación.

Bajo estas circunstancias la lectura indica 6,295,027 bytes de difusión totales, por lo que este tipo de mensajes ocupan el 90.6% de los bytes transferidos. Entonces para los nodos que generaron estos datos la comunicación principalmente se realiza mediante difusión.

El ancho de banda utilizado sólo alcanza para este caso un 0.3% de acuerdo a los 3860 bytes por segundos mostrados en la tabla correspondiente.

En términos generales, una vez revisados los datos anteriores, se deduce que la utilización de mensajes de difusión es relativamente elevado si se compara con el total de bytes presentes en la red. Si bien no se trata de una cantidad muy significativa al representar entre el 15 y 20% del total de bytes, y en un caso excepcional el 90%, al revisar las gráficas que a continuación se muestran, la información que en ellas se aprecia es que los mensajes de este tipo son constantes a lo largo del día, situación que podría reducirse.

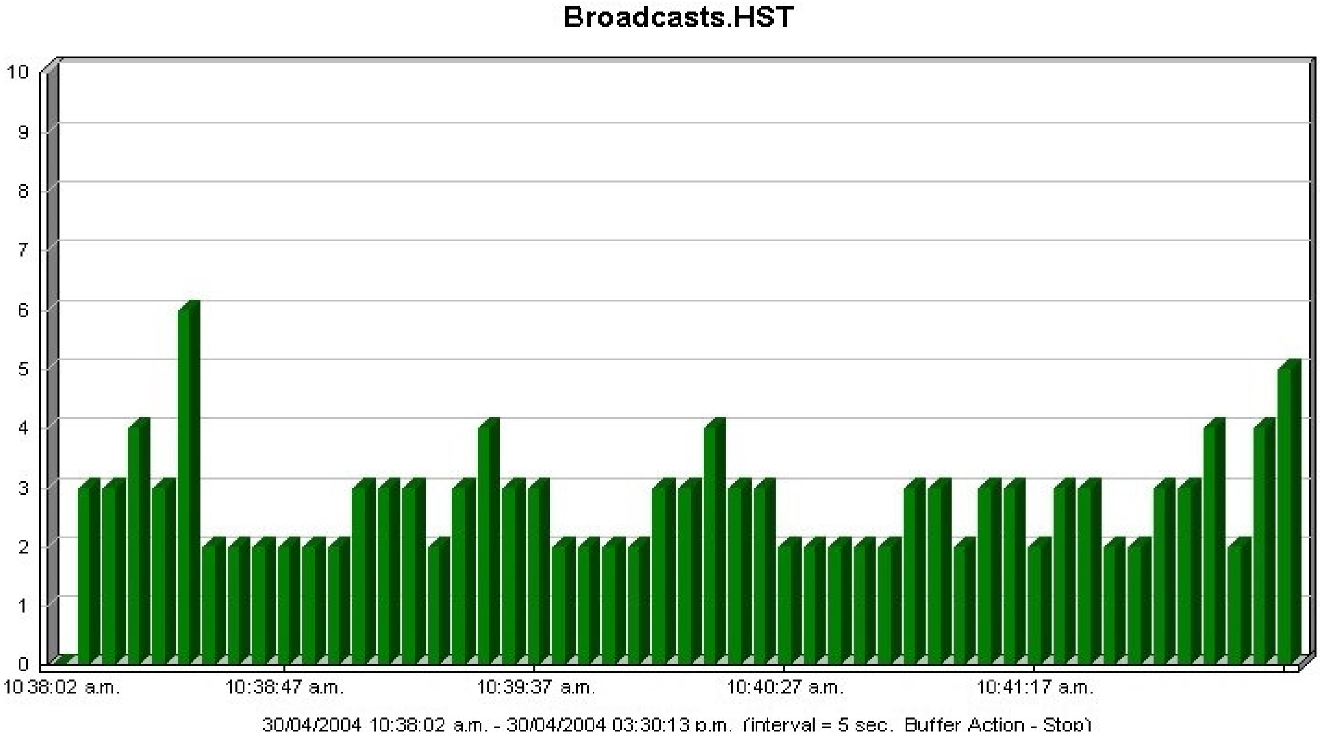

Figura 4.28 a

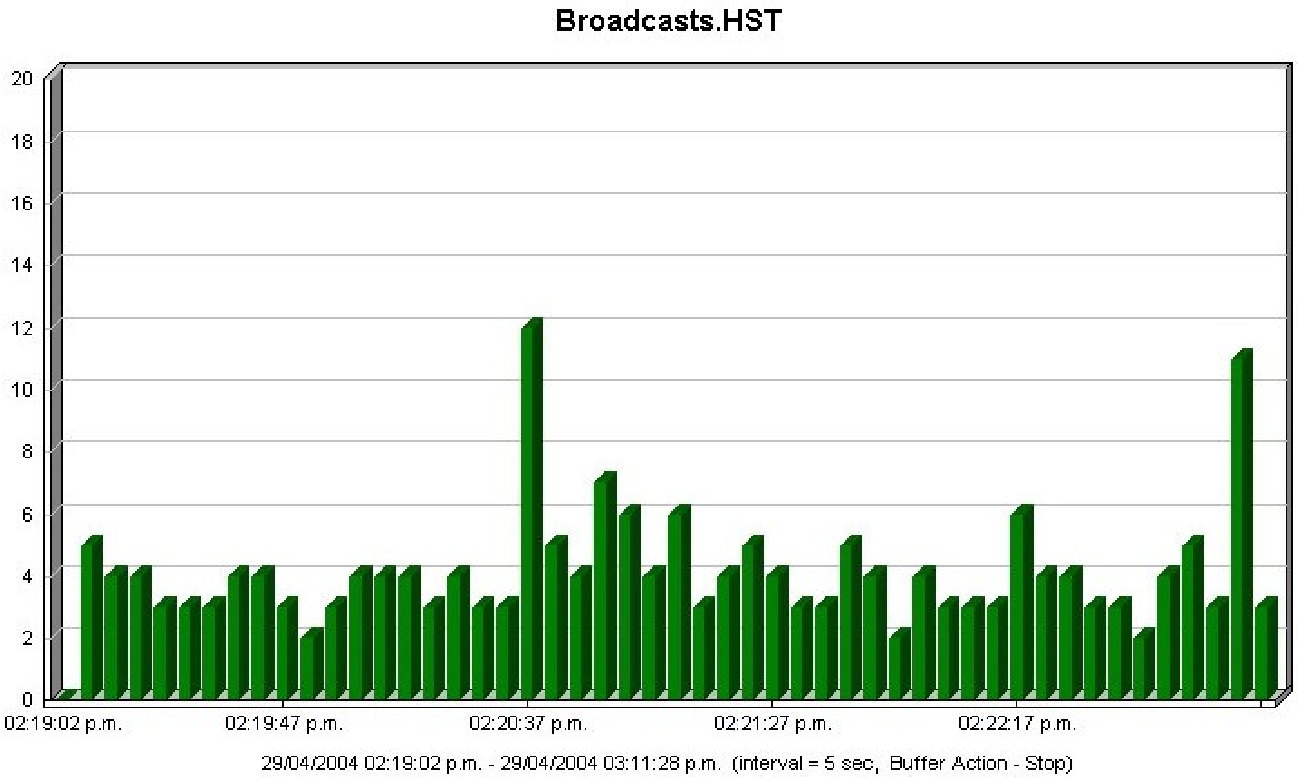

Figura 4.28 b

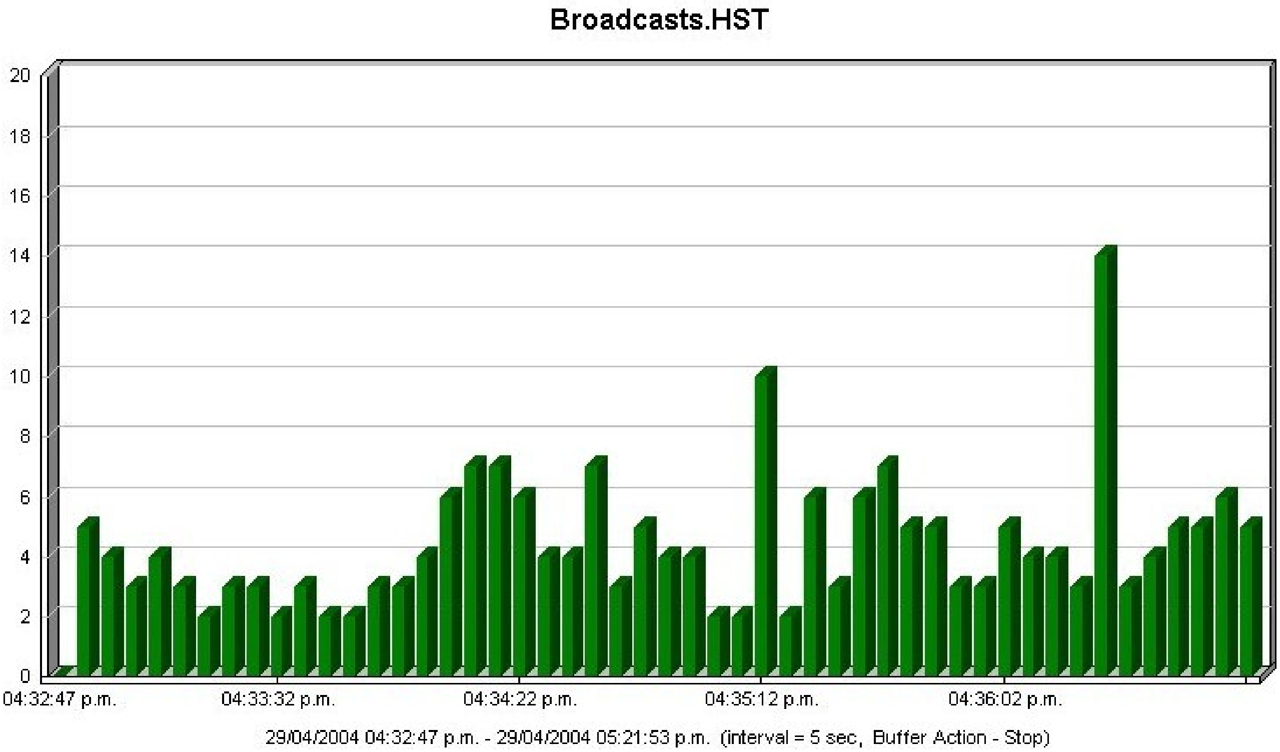

Figura 4.28 c

Figuras 4.28 a – 4.28 c: Comportamiento de la generación de mensajes de difusión.

El mayor de los inconvenientes con este tipo de mensajes se da cuando se presentan las llamadas "tormentas de difusión", en las cuales la red se inunda con mensajes de esta categoría, impidiendo la adecuada transmisión del resto de los paquetes, sobre todo cuando por instantes satura los medios de transmisión. Algunos ejemplos de situaciones de este tipo se capturaron en el contenido de las siguientes tablas:

First Time	Duration	Severity	Description	**Object**
28/4/2004 10:16:03.742	2s 267ms	Minor	Broadcast/Multicast Storm	Segment
28/4/2004 11:16:19.274	1s 831ms	Minor	Broadcast/Multicast Storm	Segment
28/4/2004 15:22:35.985	1s 56ms	Minor	Broadcast/Multicast Storm	Segment
28/4/2004 16:22:44.349	915ms	Minor	LAN overload	Segment
28/4/2004 19:25:57.759	1s 42ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 10:02:23.552	2s 43ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 14:05:34.913	1s 178ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 15:10:44.309	1s 968ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:12:35.489	923ms	Minor	LAN overload	Segment
29/4/2004 20:17:56.355	1s 174ms	Minor	Broadcast/Multicast Storm	Segment
30/4/2004 09:43:46.189	3s 183ms	Minor	Broadcast/Multicast Storm	Segment
30/4/2004 11:46:17.703	1s 51ms	Minor	Broadcast/Multicast Storm	Segment
30/4/2004 13:48:45.379	1s 975ms	Minor	Broadcast/Multicast Storm	Segment
30/4/2004 14:54:33.237	1s 204ms	Minor	LAN overload	Segment
30/4/2004 17:01:58.673	1s 74ms	Minor	Broadcast/Multicast Storm	Segment

Tabla 4.83: Ejemplos de algunos registros de detecciones de problemas sobre tormentas de difusión en un periodo de tres días, donde: First time – Primera ocasión (Inicio), Duration – Duración, Severity – Nivel de Severidad, Description – Descripción, Objet – Objeto. Para el contenido: Minor – Menor, Broadcast/Multicast Storm – Tormenta de difusión, Segment – Segmento.

First Time	Duration	Severity	Description	**Object**
29/4/2004 16:59:46.806	1s 158ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:01:19.986	961ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:02:23.552	1s 43ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:03:30.169	1s 52ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:04:46.19	934ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:05:34.913	1s 178ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:07:39.38	814ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:10:44.309	968ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:12:25.872	554ms	Minor	LAN overload	Segment
29/4/2004 17:12:35.489	923ms	Minor	LAN overload	Segment
29/4/2004 17:13:21.63	981ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:15:24.823	956ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:16:22.315	775ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:17:27.877	968ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:17:56.355	1s 174ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:19:22.483	894ms	Minor	Broadcast/Multicast Storm	Segment
29/4/2004 17:19:58.398	762ms	Minor	LAN overload	Segment

Tabla 4.84: Registros de tormentas de difusión en un periodo de aproximadamente 20 minutos.

La intención de presentar esta dos tablas es hacer notar que los casos de tormentas de difusión se hacen presentes a lo largo del día como lo muestran los datos de la tabla 4.83. Por su parte los registros de la tabla 4.84 indican que existen periodos cortos entre la ocurrencia de uno de éstos eventos y el siguiente.

Ahora, desde el punto de vista de la utilización del ancho de banda de la red LAN, la cantidad de mensajes de difusión podrían considerarse como cuestión secundaria, si se toma en cuenta que la totalidad del flujo de datos ocupa solamente como máximo un 1.85%, sin embargo no se deben pasar por alto las posibles dificultades ocasionadas por los momentos de presencia de las tormentas.

Los datos respectivos al ancho de banda se comprueban al observar las gráficas de las figuras generadas por el programa “Distinct Network Monitor”, las cuales muestran una evaluación a diferentes horas donde existen instantes en el que la utilización del ancho de banda se ve fuertemente incrementado, muy probablemente debido a las mencionadas tormentas de difusión:

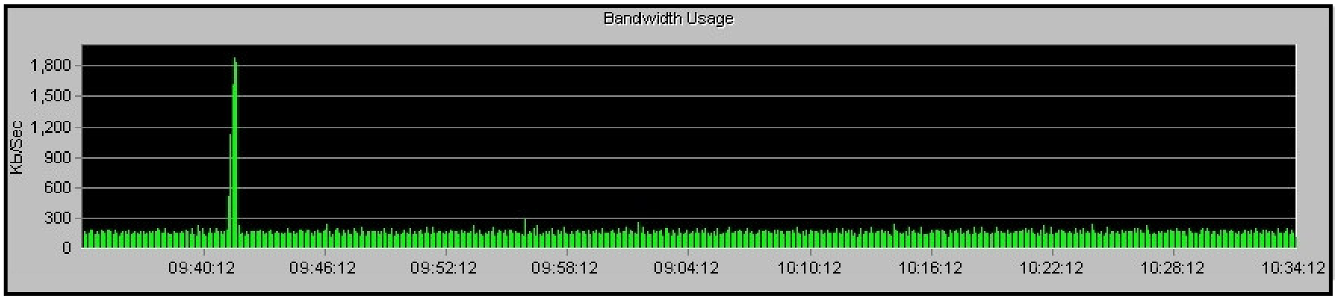

Figura 4.29 a

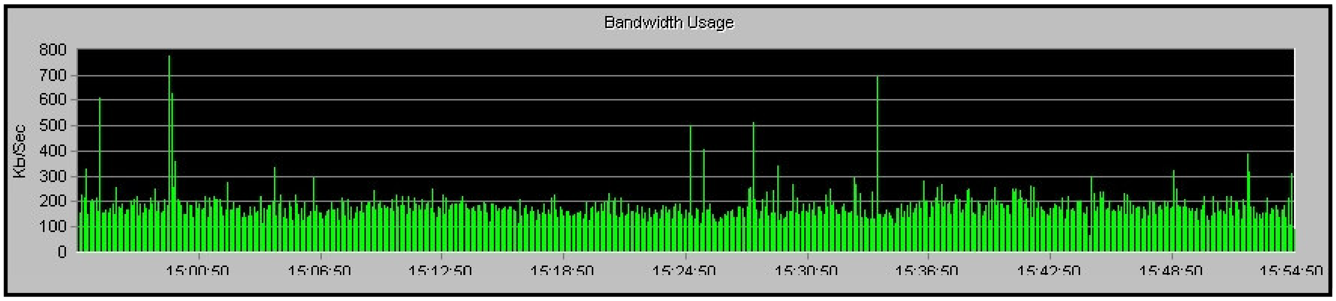

Figura 4.29 b

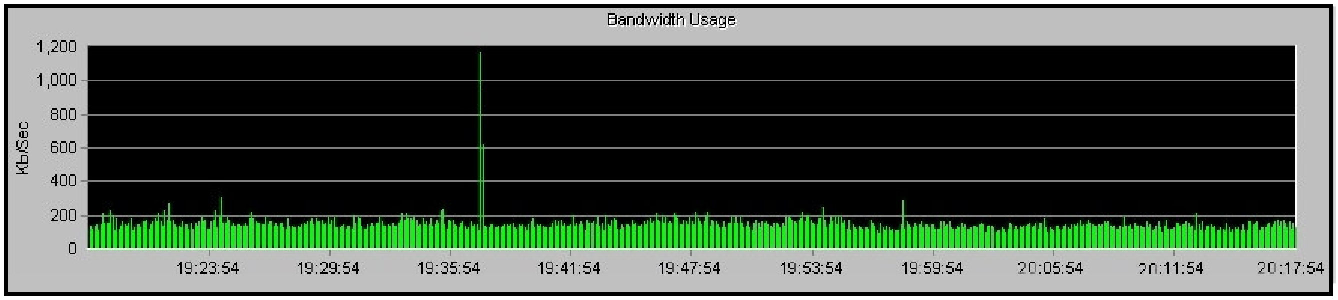

Figura 4.29 c

Figuras 4.29 a – 4.29 c: Gráficas correspondientes a la lectura de la utilización del ancho de banda.

Respecto a la disponibilidad de los servicios, aun falta analizar el aspecto referente al acceso a Internet, por lo que se requiere verificar el uso del ancho de banda proporcionado por el servicio DS0 que brinda una capacidad máxima de 64 kbps. Para tal fin se hará uso de los registros gráficos capturados por la Dirección General de Servicios de Cómputo Académico de la U.N.A.M (D.G.S.C.A.).

La primer gráfica muestra el comportamiento anual tanto de bits de entrada como de salida, correspondiendo el color verde para los primeros mientras que el azul indica los segundos. Es claro ver la disminución de la actividad entre los meses de julio y agosto, así como en el mes de diciembre, que corresponde al periodo de vacaciones de los alumnos y por tanto la baja necesaria en la demanda de los servicios. Para el resto de los meses se muestra una utilización similar entre sí.

Si se observa, para cada segmento correspondiente a un mes se aprecian cuatro picos máximos de bits salientes, que se deduce se trata de las cuatro semanas contenidas en cada mes. Los niveles bajos en los que inicia un pico y termina otro entonces deberán tratarse de los fines de semana, periodo en los que baja la actividad. En apariencia no siempre se llega al máximo de utilización del ancho de banda, sin embargo entre mayor sea el periodo de captura, los datos se vuelven menos exactos. Como se verá luego del análisis del resto de las gráficas, cuando se analiza un periodo menor los detalles respecto a los datos analizados se hacen más apreciables, pues éstos pueden pasarse desapercibidos con un mayor periodo de muestreo.

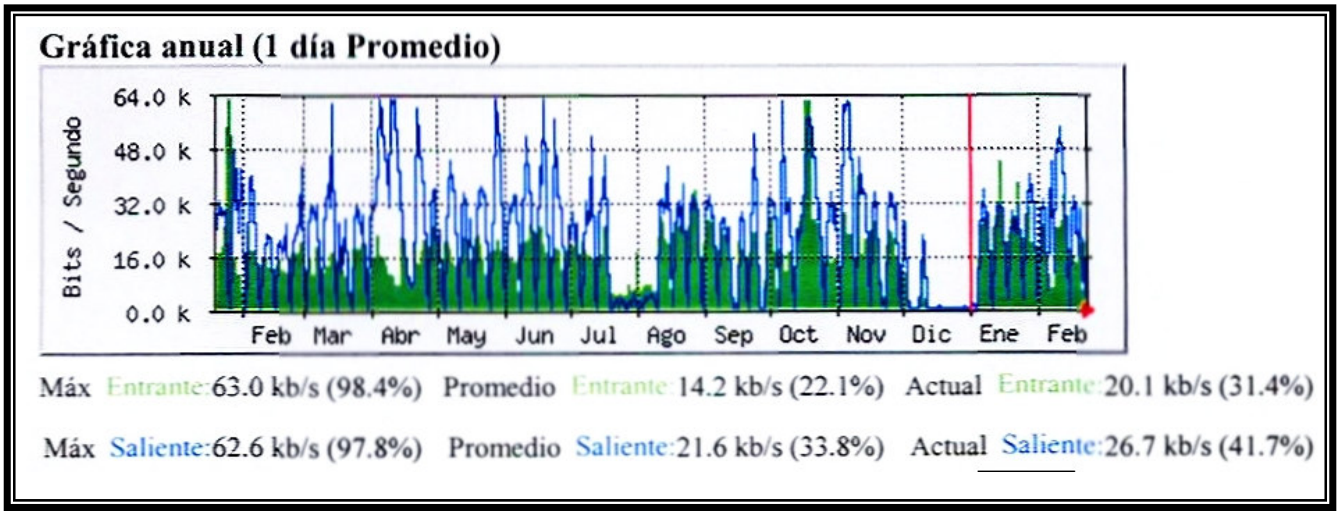

Figura 4.30 Gráfica del comportamiento anual de bits de entrada y salida respecto a la red LAN del C.C.H Vallejo

En segundo término se cuenta con la gráfica mensual, en la que se presenta un comportamiento similar a la gráfica anual, solamente que en este caso para cada segmento se cuenta con siete picos máximos, de los cuales cinco de ellos destacan en la mayoría de los casos sobre los dos restantes, mostrando así el comportamiento de los días hábiles para cada semana del mes. A diferencia de la gráfica anual los niveles de utilización, que para este caso ya son mejor apreciables, se tiene un mayor acercamiento tanto de bits de entrada como de salida hacia lo que es el máximo nivel de utilización.

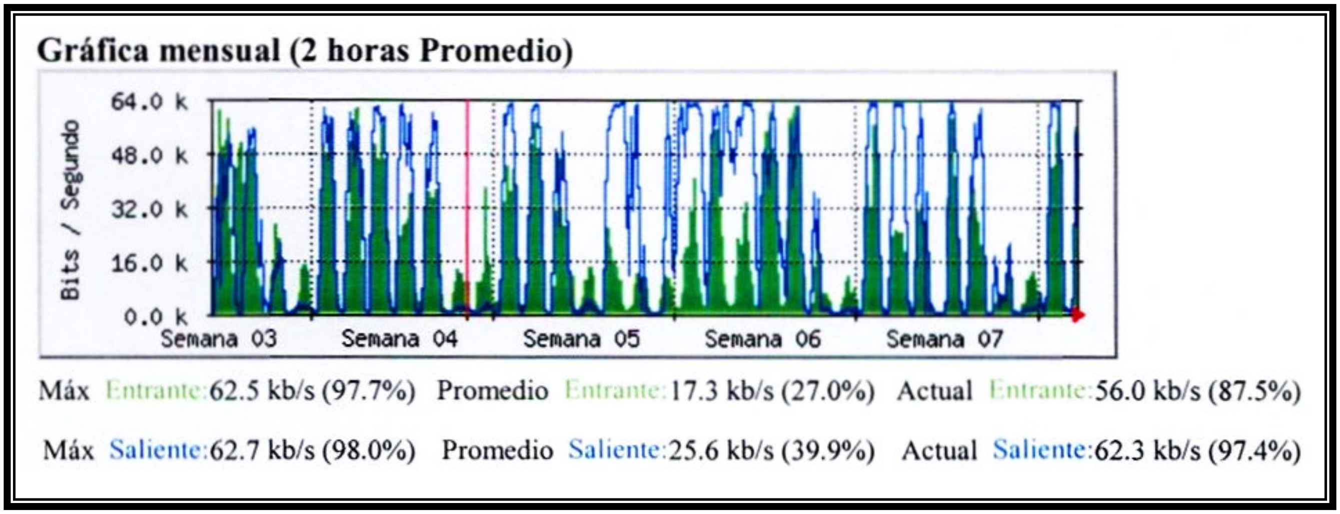

Figura 4.31 Gráfica del comportamiento mensual de bits de entrada y salida respecto a la red LAN del C.C.H Vallejo

La tercer gráfica corresponde a un análisis semanal, en donde ya es claro el verdadero comportamiento respecto al uso del ancho de banda para la salida a Internet. Los niveles de bits salientes se encuentran casi en todo momento en el máximo posible, mientras que el flujo de bits de entrada muestra en varias ocasiones picos constantes que tocan el limite de los 64 kbps.

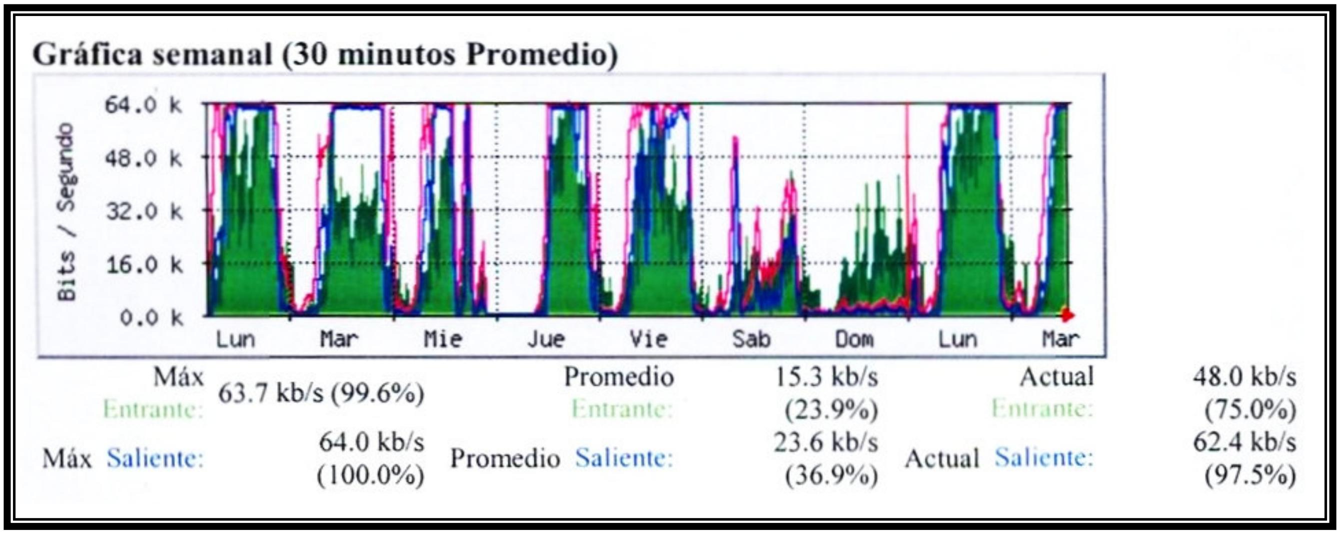

Figura 4.32 Gráfica del comportamiento semanal de bits de entrada y salida respecto a la red LAN del C.C.H Vallejo

Finalmente se presenta un caso particular mostrando el uso del ancho de banda a lo largo de las horas respectivas de un día en específico. Se tiene que la actividad está comprendida entre las 8:00 y las 22:00 horas, periodo en el que el flujo de bits de salida se muestra constante y prácticamente en todo instante en el límite superior, en tanto que el tránsito de los bits de entrada se encuentra por encima de los 32 kbps con picos frecuentes que se acercan al máximo, sobre todo hacia el final del periodo de mayor actividad.

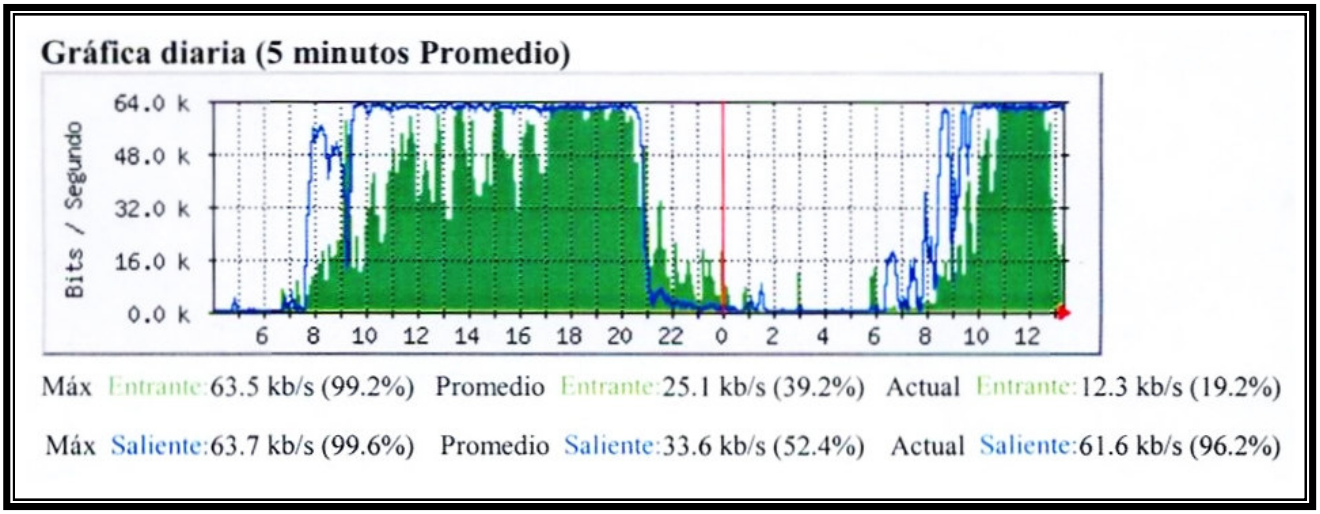

Figura 4.33 Gráfica del comportamiento diario de bits de entrada y salida respecto a la red LAN del C.C.H Vallejo

De acuerdo a las estadísticas que acompañan a las gráficas, se indica que en promedio el flujo de datos entrante va desde 14.2 kbps equivalentes al 22.1%, hasta 25.1 kbps que se traducen en un 39.2% del ancho de banda. Por su parte, el comportamiento de los bits de salida va desde 21.6 kbps correspondientes al 33.8%, hasta 33.6 kbps (52.4%). Pese a lo que indican estos datos, es más adecuado tomar como referencia lo mostrado en las gráficas considerando los periodos en los que se hace uso de la red, con el fin de llegar a una buena conclusión respecto a la carga del ancho de banda, ya que estas estadísticas fueron generadas considerando incluso los periodos de inactividad de los usuarios, por tanto considerar estos indicativos como niveles reales de utilización sería caer en un error.

De esta forma, se tiene que considerando únicamente el periodo efectivo de utilización, tratándose de esto lo que realmente se necesita analizar, claramente se observa que la utilización del ancho de banda, según lo descrito para las dos últimas gráficas, se encuentra en sus niveles máximos prácticamente en todo instante, lo que necesariamente lleva a la conclusión de que en esta red se ha alcanzado un nivel de saturación en el que la disponibilidad del servicio de conexión a Internet ya es muy baja, sentencia que no solamente está justificada por lo anteriormente explicado, sino además por la cantidad de usuarios a los que se les debe atender las demandas de servicio haciendo uso únicamente de los ya citados 64 kbps.

Identificación de “cuellos de botella”.

De acuerdo a lo expuesto en los dos temas anteriores se facilita la identificación de los puntos de la red donde se presentan los “cuellos de botella”, secciones en las cuales, como se dado aconocer con anterioridad, se dificulta el flujo de información.

El estudio de las colisiones mostró no ser un gran inconveniente, y considerando además que la ocupación del ancho de banda interno no excede el 2%, se concluye entonces que las tramas circulan sin mayores problemas en el dominio de la red LAN. Sin embargo no se presenta la misma situación para paquetes que pretenden entrar o salir de la red local.

Retomando el estudio correspondiente a las retransmisiones de las sesiones TCP, la gran problemática en este caso se trataba de los paquetes de entrada y salida, es decir los que involucran a un nodo exterior a la red.

Complementando esto con los resultados mostrados respecto a la utilización del ancho de banda para conexión WAN, es notorio que en este punto se tiene una de las situaciones en cuestión de “cuello de botella”, ya que como indica el número de retransmisiones en muchos de los casos no es posible hacer una transmisión adecuada debido a la saturación del canal. El número de paquetes que el enrutador descarta ante la imposibilidad de procesarlos debe tratarse de una cantidad considerable, que como consecuencia afecta la disponibilidad de servicio considerando los inconvenientes mencionados.

Administración.

Un aspecto que no deja de ser importante para el correcto desempeño de una red es la manera en que ésta se encuentra administrada, debido a que la solución a problemas será más rápida en cuanto menor tiempo se requiera para la detección de situaciones indeseables.

El caso que se está estudiando cuenta con una administración que soluciona las dificultades solamente sobre aviso por parte de los usuarios, esto es, que los administradores no cuentan con programas específicos de análisis de redes para la lectura del desempeño, por lo que únicamente reciben notificaciones verbales referentes a problemas, en su mayoría por falta de servicio.

En lo que respecta a la administración del único enrutador, es la D.G.S.C.A. quien se encarga de la observación de este equipo, enfocándose sobre todo a la generación de las estadísticas respecto al flujo de bits de entrada y salida.